DEFORMAÇÕES DE REPRESENTAÇÕES GALOISIANAS ORDINÁRIAS E DE REPRESENTAÇÕES NÃO RAMIFICADAS

Paulo Agozzini Martin

TESE APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA OBTENÇÃO DO GRAU DE DOUTOR EM MATEMÁTICA

ORIENTADOR: **Prof. Dr. Fernando Quadros Gouvea**

São Paulo, setembro de 1991

A Fernando Quadros Gouvea,

com amizade.

ABSTRACT

In this thesis we treat two problems concerning deformations of a continuous residual Galois representation

$$(*), \qquad \overline{\rho} : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(k)$$

which are unramified outside some finite set S of primes containing the characteristic p of the finite field k.

Essentially, a deformation of $\overline{\rho}$ is a lift ρ of $\overline{\rho}$, $\rho : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(A)$, where A is a complete Noetherian local ring with residue field k. Mazur, [Ma1], showed that the set of such liftings of $\overline{\rho}$ can be parametrized by a ring $\mathbf{R}(\overline{\rho})$ in the same category as A (provided $\overline{\rho}$ be absolutely irreducible). If we fix a certain behavior of an inertia subgroup I at p in a representation

$$\rho : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(A),$$

namely, the set of invariant elements in $A \times A$ fixed by I is a A–submodule free of rank 1 and a direct sommand, we say that ρ is an ordinary representation. For an ordinary representation (*) Mazur, [Ma1], showed that all ordinary liftings are likewise parametrized by a ring $\mathbf{R}^0(\overline{\rho})$.

The first problem we treat is to find ordinary deformations of a residual representation (*), which is *unramified at* p. In this case, the ring $\mathbf{R}^0(\overline{\rho})$ no longer exists, although there are ordinary liftings of $\overline{\rho}$. We do this in case $\overline{\rho}$ is a special dihedral representation (cf. Chapter II) and the set S of primes is $S = \{\ell, p, \infty\}$ and considering deformation to the ring of p–adic integers $\mathbf{Z}_p$. This is done in Chapter II.

The second problem is to consider an ordinary residual representation $\overline{\rho}$ and to analyse the natural map

$$\mathbf{R}(\overline{\rho}) \to \mathbf{R}^0(\overline{\rho}).$$

We prove that this map is surjective and under mild hypothesis that its kernel can be generated by two generators, thus generalizing a similar result of Mazur, [Ma2].

ÍNDICE

INTRODUÇÃO

Em [Ma1], Mazur introduziu o estudo das deformações de uma representação Galoisiana residual

$$\overline{\rho} : G \to GL_2(k),$$

onde G é o grupo de Galois absoluto de um corpo local de característica zero ou o grupo de Galois da maior extensão de um corpo de números, não ramificada fora de um conjunto finito S de primos, e k é um corpo finito de característica p. Uma deformação de $\overline{\rho}$ é um levantamento $\rho : G \to GL_2(A)$, onde A é um anel local Noetheriano completo cujo corpo de restos é k, tal que o diagrama óbvio comuta:

$$\begin{array}{ccc} & & GL_2(A) \\ & \rho \nearrow & \\ G & & \downarrow \\ & \overline{\rho} \searrow & \\ & & GL_2(k) \end{array}$$

Na verdade, vamos identificar duas tais ρ's que forem conjugadas por um elemento do kernel da redução canônica $GL_2(A) \to GL_2(k)$, chamando de deformação de $\overline{\rho}$ a toda a classe de equivalência de ρ.

No artigo citado, Mazur provou que o functor

$$F : C(k) \to \text{Conjuntos}$$

onde $C(k)$ é a categoria dos anéis locais Noetherianos completos com corpo de restos k, e $F(A) = \{\text{deformações de } \overline{\rho} \text{ para } GL_2(A)\}$ é representável, desde que $\overline{\rho}$ seja absolutamente irredutível. Ou seja, nesse caso existe um anel $\mathbf{R}(\overline{\rho})$ em $C(k)$ e uma deformação $\rho^u : G \to GL_2(\mathbf{R}(\overline{\rho}))$ tal que qualquer deformação de $\overline{\rho}$ para qualquer anel A de $C(k)$ é obtida de um único morfismo $\mathbf{R}(\overline{\rho}) \to A$.

Se $\overline{\rho}$ não for absolutamente irredutível, ainda assim existem $\mathbf{R}(\overline{\rho})$ e ρ^u como acima, porém o morfismo $\mathbf{R}(\overline{\rho}) \to A$ não é necessariamente único. Podemos pensar em $X = \mathrm{Spec}(\mathbf{R}(\overline{\rho}))$ como o espaço das deformações de $\overline{\rho}$, pois seus pontos são justamente os morfismos $\mathbf{R}(\overline{\rho}) \to A$. Mazur obteve vários resultados sobre a estrutura de $\mathbf{R}(\overline{\rho})$ e sobre interessantes propriedades geométricas de X em casos particulares. Uma das questões importantes colocadas por Mazur é saber se as deformações de uma representação $\overline{\rho}$ associada a uma forma modular são também associadas a formas modulares. Para clarificar esse ponto, recordamos que Deligne mostrou [De] como associar a uma forma modular parabólica f em $\Gamma_1(N)$, que seja autofunção dos operadores de Hecke, uma representação Galoisiana

$$\rho_f : Gal(\overline{Q}/Q) \to GL_2(k)$$

com certas propriedades especiais. (Veja adiante, em I-4, um enunciado preciso). Serre [Serre] conjecturou a recíproca desse teorema. Assim, nesse contexto, se $\overline{\rho}$ for uma representação residual que está associada a uma forma modular via o teorema de Deligne, faz sentido perguntar se todas as deformações de $\overline{\rho}$ são também associadas a formas modulares. Nesta situação, necessariamente entram em cena as formas modulares p–ádicas. Para essas e para o problema em questão, consultar especialmente [Gou1] e as referências ali citadas. Entre outras coisas, o capítulo III de [Gou1] destina-se à construção de representações Galoisianas associadas a formas modulares p–ádicas e a mostrar que uma boa parte das deformações de $\overline{\rho}$ está de fato associada a formas modulares p–ádicas. Hida, [H1], [H2], foi o primeiro a observar que é possível associar representações p–ádicas a formas modulares p–ádicas. No caso das representações associadas a formas modulares p–ádicas ordinárias (veja as referências acima para definições, e também I-4 adiante), Mazur e Wiles, [M-W], estudaram a construção de Hida do ponto de vista geométrico e construíram uma família de deformações de uma representação (suposta absolutamente irredutível e associada a uma forma modular ordinária) que parametriza todas as possíveis deformações associadas a formas modulares p–ádicas ordinárias. Nesse mesmo artigo, eles

mostram que se $\rho : G \to GL_2(A)$ é um elemento dessa família (A um anel de $C(k)$, k corpo finito de característica p), então o conjunto dos elementos de $A \times A$ fixos pelo subgrupo de inércia em p, é um A–submódulo livre de posto 1 e somando direto de $A \times A$. Portanto, na procura de associar formas modulares e representações, surge a necessidade de se considerar representações Galoisianas ordinárias – aquelas que possuem a propriedade enunciada acima – de modo independente, como faz Mazur em [Ma 1]. Se começamos com uma representação residual

$$\overline{\rho} : G \to GL_2(k)$$

que seja ordinária, faz sentido procurarmos deformações de $\overline{\rho}$ que também sejam ordinárias. Mazur provou que o functor

$$F^0 : C(k) \to \text{Conjuntos}$$

que a cada anel A de $C(k)$ associa o conjunto das deformações ordinárias de $\overline{\rho}$ para $GL_2(A)$ é representável por um anel $\mathbf{R}^0(\overline{\rho})$ em $C(k)$. A conjectura é que esse anel (no caso de $\overline{\rho}$ estar associada a uma forma modular) é o anel que parametriza todas as representações associadas a formas modulares p–ádicas ordinárias anteriormente citado.

Esse paralelismo (em parte conjectural) entre os anéis universais $\mathbf{R}(\overline{\rho})$, $\mathbf{R}^0(\overline{\rho})$ e os anéis associados a representações oriundas de formas p–ádicas e formas p–ádicas ordinárias nos leva a esperar certas propriedades especiais do morfismo natural (que vem da universalidade de $\mathbf{R}(\overline{\rho})$):

$$(*) \qquad \mathbf{R}(\overline{\rho}) \to \mathbf{R}^0(\overline{\rho}).$$

(a) O morfismo $(*)$ é sobrejetor.

(b) O kernel de $(*)$ pode ser gerado por dois elementos.

Em [Ma 1], Mazur provou (a) e (b) para uma classe bastante particular de representações residuais e em [Ma 2], Mazur provou (a) e (b) para representações residuais $\overline{\rho} : G \to GL_2(k)$ tais que $\det\overline{\rho} \neq 1$, ω, ω^{-1}, $\omega^{(p-1)/2}$, onde ω é o carácter ciclotônico.

No Capítulo III nós provamos (a) em completa generalidade e (b) no caso em que o corpo recortado por $\overline{\rho}$ não possui inércia selvagem. Mais precisamente, provamos o

Teorema. Seja $\overline{\rho} : Gal(\overline{Q}/Q) \to GL_2(k)$ uma representação contínua, absolutamente irredutível, ordinária, não ramificada fora de $S = \{p, \infty\}$, então o morfismo natural $\mathbf{R} \to \mathbf{R}^0$ é sobrejetor. Se $\overline{\rho}$ for moderadamente ramificada, seu kernel pode ser gerado por dois elementos.

Salientamos que a hipótese de $\overline{\rho}$ ser moderadamente ramificada implica que $\det\overline{\rho} \neq 1$, mas os demais casos podem ocorrer. Salientamos também que nossas técnicas são absolutamente diferentes das de Mazur, no sentido de que a utilização da teoria dos corpos de classe nos permitiu uma abordagem mais conceitual e intrínseca do problema.

No Capítulo II tratamos de um problema ligeiramente diferente. Consideramos uma representação Galoisiana residual

$$\overline{\rho} : Gal(\overline{Q}/Q) \to GL_2(k)$$

(onde como sempre k é um corpo finito de característica p) que não ramifica em p – e portanto não pode ser ordinária. Tais representações surgem naturalmente de formas modulares de peso 1 (via o teorema de Deligne-Serre). É claro que $\overline{\rho}$ vai ramificar em outros primos e portanto as deformações de $\overline{\rho}$ serão não ramificadas fora de $S = \{\ell_1, \ldots, \ell_n, p, \infty\}$. Neste caso, o anel universal $\mathbf{R}^0(\overline{\rho})$ das deformações ordinárias não existe mais, pois o functor

$$F^0 : C(k) \to \text{Conjuntos}$$

não é representável.

Porém, existem deformações ordinárias em $X = \text{Spec}(\mathbf{R}(\overline{\rho}))$,

> *"(...) and it would be very interesting to understand this situation better. For example, will the locus of ordinary deformations in* $X = \text{Spec}(\mathbf{R})$ *be a subscheme?"* [Gou2].

Guiados por essa pergunta, procuramos respondê-la para uma certa classe de representações residuais $\overline{\rho}$.

Em [Ma 1], Mazur introduziu uma classe de representações (special–dihedral S_3–representations) obtidas essencialmente de uma extensão de Galois L/Q cujo grupo de Galois é S_3 (o grupo simétrico em 3 letras) e que é corpo de decomposição de um polinômio da forma $f(X) = X^3 + aX + 1$ para inteiros a tais que $27 + a^3$ seja um primo ℓ. E Mazur estudou deformações das representações residuais associadas

$$\overline{\rho} : Gal(\overline{Q}/Q) \to GL_2(\mathbf{F}_\ell)$$

onde $S = \{\ell, \infty\}$.

Nós consideramos as representações associadas a essas extensões L/Q, mas num corpo finito de característica $p \neq \ell$,

$$\overline{\rho} : Gal(\overline{Q}/Q) \to GL_2(\mathbf{F}_p)$$

com $S = \{p, \ell, \infty\}$. Neste caso, $\overline{\rho}$ é não ramificada em p, e a determinação do anel universal das deformações já não é tão simples (sobretudo no caso em que $x^3 + ax + 1$ é irredutível mod p), e provamos o seguinte teorema:

Teorema 1. Seja $\overline{\rho} : G_{Q,\{p,\ell,\infty\}} \to GL_2(\mathbf{F}_p)$ uma representação especial e L/Q o seu corpo de decomposição. Então se $p \nmid (\ell - 1)$ e p não dividir o número de classes de $L(\zeta_p)$ onde ζ_p é uma raiz p-ésima da unidade, o grupo de Galois P da maior pro–p–extensão de L não ramificada fora de $\{p, \ell, \infty\}$ é livre em 4 geradores.

Com esse teorema, por um simples argumento de cohomologia podemos mostrar que

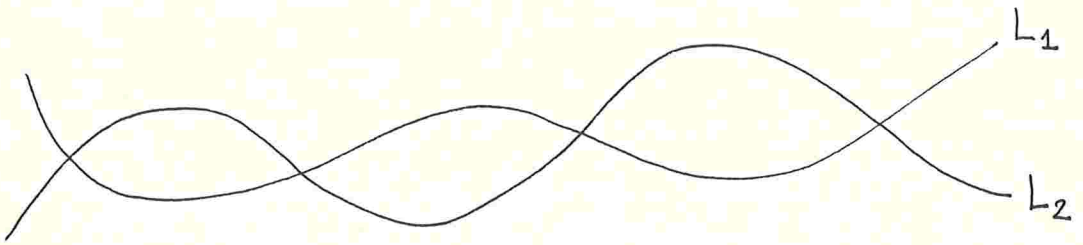
$$\mathbf{R}(\overline{\rho}) \cong \mathbf{Z}_p[[T_1, T_2, T_3]]$$

e usando as técnicas desenvolvidas por Boston, [Bo], e Mazur, [Bo-Ma], achamos a deformação universal explicitamente, e passamos a procurar deformações ordinárias em

$X = \mathrm{Spec}(\mathbf{R}(\overline{\rho}))$. Na verdade, restringimos o problema, procurando deformações ordinárias em $\mathbf{Z}_p$, o anel de inteiros p–ádicos, pois nesse caso

$$X_p = \mathrm{Hom}(\mathbf{R}(\overline{\rho}), \mathbf{Z}_p)$$

é naturalmente uma variedade analítica p–ádica tridimensional, e podemos dar uma descrição razoável do subconjunto $X_p^0 \subseteq X_p$ dos pontos ordinários:



$X_p^0 = (L_1 \backslash (L_1 \cap L_2)) \cup (L_2 \backslash (L_1 \cap L_2))$. Onde $L_1 \cap L_2$ é o conjunto dos pontos não ramificados de X_p (i.e., correspondem a deformações para $GL_2(\mathbf{Z}_p)$ que não ramificam nem em p nem em ℓ). Assim, X_p^0 não é um subesquema–fechado de X_p.

CAPÍTULO I

DEFORMAÇÕES DE REPRESENTAÇÕES GALOISIANAS

I-1 – Deformações Universais

Seja k um corpo finito de características p e $C(k)$ a categoria cujos objetos são anéis locais Noetherianos completos cujo corpo de restos é k e cujos morfismos são homomorfismos de anéis locais induzindo a identidade nos corpos de restos. Se R é um anel local em $C(k)$ e m_R é o seu ideal maximal, definimos o **espaço cotangente** de R por:

$$t_R^* = m_R/(m_R^2 + pR).$$

É bem conhecido que um tal R será um quociente do anel $W(k)[[T_1, \ldots, T_r]]$, onde $r = \dim_k t_R^*$ e $W(k)$ é o anel de vetores de Witt de k (cf. por exemplo [Bour], IX.27, Teor.3).

Se G for um grupo profinito, diremos que G satisfaz a condição de finitude (Φ_p) se para todo subgrupo aberto H de G, valerem as seguintes condições equivalentes:

(a) O maior pro–p–quociente abeliano de H é finitamente gerado.

(b) O maior quociente p–abeliano elementar de H é finitamente gerado.

A classe dos grupos profinitos que satisfazem a condição de finitude (Φ_p) para *todo primo* p será denotada Φ. Φ contém os seguintes grupos:

(1) O grupo de Galois absoluto $\mathrm{Gal}(\overline{K}/K)$ de um corpo local de característica zero (cf. [Koch], §10).

(2) O grupo de Galois $\mathrm{Gal}(L/K)$ da maior extensão L de um corpo de números K não ramificada fora de um dado conjunto finito S de primos de K (cf. [Koch], §11).

(3) Mais geralmente, o grupo fundamental algébrico $\pi_1^{\text{alg}}(X, \overline{x})$, onde X é um esquema de tipo finito sobre $\mathbf{Z}$, geometricamente conexo e liso, e $\overline{x}$ é um ponto geométrico de X (cf. [K-L]).

Como estamos interessados nos grupos do tipo (1) e (2) acima, vamos escrever G_K para um grupo profinito como em (1) e $G_{K,S}$ para um grupo como em (2).

Seja n um inteiro positivo. Se G for um grupo profinito satisfazendo a condição de finitude (Φ_p) e A for um anel local em $C(k)$, dois homomorfismos contínuos de G em $GL_n(A)$ são ditos *estritamente equivalentes* se um puder ser levado no outro através da conjugação por um elemento no kernel da redução canônica $GL_n(A) \to GL_n(k)$.

Por uma *representação* de G em $GL_n(A)$ entenderemos uma classe de equivalência estrita de um homomorfismo contínuo de G em $GL_n(A)$. Assim, se $A = k$, uma representação nada mais é que um homomorfismo contínuo. Por abuso de linguagem escreveremos "$\rho : G \to GL_n(A)$", onde ρ é uma representação.

Se $A_1 \to A_2$ for um morfismo na categoria $C(k)$ e se ρ_1 e ρ_2 forem representações de G em $GL_n(A_1)$ e em $GL_n(A_2)$ respectivamente, diremos que ρ_1 é uma *deformação* de ρ_2 se qualquer homomorfismo de G em $GL_n(A_1)$ na classe de equivalência estrita ρ_1, quando composto com o homomorfismo induzido $GL_n(A_1) \to GL_n(A_2)$, fornecer um homomorfismo na classe de equivalência estrita ρ_2.

Por uma *representação residual de dimensão* n (num contexto em que G e k estiverem claros) entenderemos um homomorfismo contínuo

$$\overline{\rho} : G \to GL_n(k)$$

i.e., uma representação de G em $GL_n(k)$.

Fixemos G e k como acima. O teorema que enunciaremos a seguir estabelece a existência de uma deformação universal de qualquer representação residual n–dimensional absolutamente irredutível $\overline{\rho}$. Mais precisamente, existe um anel local Noetheriano com-

pleto $\mathbf{R} = \mathbf{R}(G, k, \overline{\rho})$ cujo corpo de restos é k, e uma deformação de $\overline{\rho}$

$$\rho^u : G \to GL_n(\mathbf{R}),$$

que é universal no sentido de que para todo $A \in C(k)$ e toda deformação ρ de $\overline{\rho}$ para A, existe um único homomorfismo $\mathbf{R} \to A$ em $C(k)$ tal que o homomorfismo induzido $GL_n(\mathbf{R}) \to GL_n(A)$ leva ρ^u em ρ. O par $(\mathbf{R}, \rho^u)$ é determinado a menos de isomorfismo canônico. O anel local $\mathbf{R} = \mathbf{R}(G, k, \overline{\rho})$ será chamado *o anel universal das deformações de* $\overline{\rho}$ e Spec $\mathbf{R}$ será chamado o *espaço universal das deformações de* $\overline{\rho}$.

Teorema 1 (Mazur). *Existência e Unicidade.* (a) se $\overline{\rho}$ for absolutamente irredutível existem o anel universal $\mathbf{R} = \mathbf{R}(G, k, \overline{\rho})$ e a deformação universal ρ^u de $\overline{\rho}$. O par $(\mathbf{R}, \rho^u)$ é univocamente determinado a menos de isomorfismo canônico. (b) Se $\overline{\rho}$ não for absolutamente irredutível, então existe uma deformação "versal" de $\overline{\rho}$, i.e., existe uma envolvente (hull) no sentido de Schlessinger, [Sch], o que significa que podemos encontrar um objeto $\mathbf{R}$ de $C(k)$ e uma deformação ρ de $\overline{\rho}$ para $\mathbf{R}$ tal que qualquer deformação ρ_0 de $\overline{\rho}$ para qualquer anel A em $C(k)$ é induzida por um morfismo $\mathbf{R} \to A$ não necessariamente único.

A prova desse teorema pode ser encontrada em [Ma 1], bem como várias propriedades fundamentais de $\mathbf{R} = \mathbf{R}(G, k, \overline{\rho})$. Para uso posterior citaremos apenas duas propriedades:

(a) Fixemos G e k, e seja

$$\delta_{/W(k)} : GL_{n/W(k)} \to GL_{m/W(k)}$$

um homomorfismo de esquemas–grupo. Consideremos a representação residual

$$\overline{\rho} : G \to GL_n(k)$$

e seja $\overline{\rho}'$ a composta de $\overline{\rho}$ com $\delta/W(k)$. Essa composição leva deformações de $\overline{\rho}$ em deformações de $\overline{\rho}'$. Se $\overline{\rho}$ e $\overline{\rho}'$ forem absolutamente irredutíveis e

$\mathbf{R} = \mathbf{R}(G, k, \overline{\rho})$, $\mathbf{R}' = \mathbf{R}'(G, k, \overline{\rho}')$ forem os anéis universais, então teremos um homomorfismo induzido

$$\pi(\delta) : \mathbf{R}' \to \mathbf{R}$$

na categoria $C(k)$. Em particular, se

$$\delta_g : GL_{n/W(k)} \to GL_{n/W(k)}$$

for dado pela conjugação por um elemento fixo $g \in GL_n(W(k))$ obtemos um isomorfismo em $C(k)$:

$$r(\delta_g) : \mathbf{R}(G, k, \overline{\rho}') \xrightarrow{\cong} \mathbf{R}(G, k, \overline{\rho})$$

onde $\overline{\rho}'$ é a representação residual equivalente a $\overline{\rho}$ (mas não no sentido estrito) obtida por conjugação via a redução de g, $\overline{g} \in GL_n(k)$.

(b) Seja $\overline{\rho}$ uma representação absolutamente irredutível e

$$\delta = \det : GL_{n/W(k)} \to GL_{1/W(k)}$$

o homomorfismo determinante. Temos então um morfismo

$$\mathbf{R}(G, k, \det\overline{\rho}) \to \mathbf{R}(G, k, \overline{\rho})$$

e o anel $\mathbf{R}(G, k, \det\overline{\rho})$ pode ser descrito como segue: pomos $\Gamma = G^{ab,p}$, onde $G^{ab,p}$ é o p–completamento abealianizado de G (veja I-3 para as definições) e

$$\Lambda = W(k)[[\Gamma]] = \varprojlim W(k)[\Gamma/\Gamma'],$$

onde Γ' é subgrupo aberto normal de Γ.

Tem-se $\Lambda \cong \mathbf{R}(G, k, \det\overline{\rho})$, e portanto o morfismo acima dá ao anel $\mathbf{R} = \mathbf{R}(G, k, \overline{\rho})$ uma estrutura de Λ–álgebra.

I-2 - Representações Ordinárias

Fixemos G e k e um subgrupo fechado I de G. Uma representação *bidimensional*

$$\rho : G \to GL_2(A) \quad (A \in C(k))$$

é dita ordinária em I se para $M = A \times A$ com a estrutura de G–módulo dada por um homomorfismo na classe de equivalência estrita de ρ composto com a ação canônica de GL_2 em M, o sub–A–módulo $M^I \subset M$ dos elementos fixos por I for um somando direto de M, livre e de posto 1 sobre A.

Se o subgrupo I de G ficar subentendido (como por exemplo no caso em que G é o grupo de Galois da maior extensão de um corpo de números K, não ramificada fora de um conjunto finito de primos contendo p – como sempre p é a característica de k e I é o subgrupo de inércia em p) diremos simplesmente que ρ é ordinária. Suponhamos que a nossa representação residual

$$\overline{\rho} : G \to GL_2(k)$$

seja ordinária e que procuremos deformações de $\overline{\rho}$ que também sejam ordinárias. Temos o análogo do teorema 1:

Teorema 2. Se $\overline{\rho}$ for uma representação residual ordinária, absolutamente irredutível, então existe uma deformação ordinária universal de $\overline{\rho}$, isto é, existe um anel local em $C(k)$, $\mathbf{R}^0 = \mathbf{R}^0(G, k, \overline{\rho})$ e uma deformação ordinária ρ^0 de $\overline{\rho}$ para $\mathbf{R}^0$ tal que qualquer deformação ordinária de $\overline{\rho}$ para qualquer anel local A de $C(k)$ é induzida de ρ^0 via um único morfismo $\mathbf{R}^0 \to A$.

Como no caso do teorema 1, a prova desse teorema é uma aplicação quase imediata do critério de representabilidade de Schlessinger (cf. [Sch]). O anel $\mathbf{R}^0 = \mathbf{R}^0(G, k, \overline{\rho})$ é chamado o *anel universal das deformações ordinárias de* $\overline{\rho}$ e ρ^0 é chamada *a deformação ordinária universal.*

É claro que existe um morfismo natural

$$\mathbf{R}(G,k,\overline{\rho}) \to \mathbf{R}^0(G,k,\overline{\rho})$$

que se obtém pela universalidade de $\mathbf{R}$. Uma das razões principais para o estudo do anel $\mathbf{R}^0$ vem da sua relação (em sua maior parte conjectural) com formas modulares, tema que será abordado em I-4.

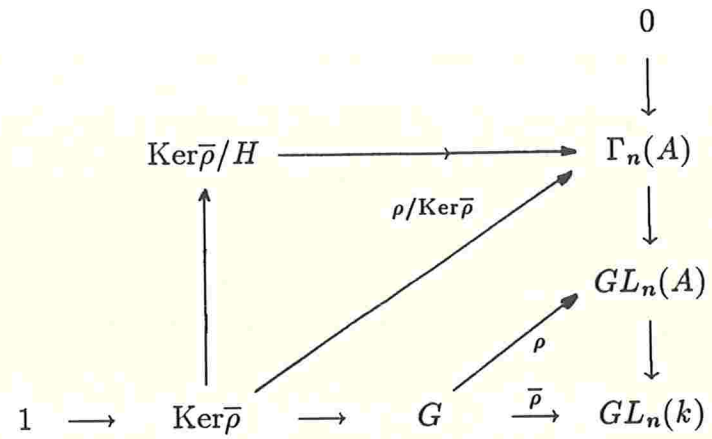
I-3 - Deformações Explícitas

Este parágrafo destina-se à apresentação de um método que possibilita, em alguns casos, calcular explicitamente a deformação universal de certas representações residuais. Todos os resultados aqui apresentados serão utilizados na demonstração do teorema principal do Capítulo III, e podem ser vistos com mais detalhes na tese de N. Boston, [Bo].

Se A for um anel de $C(k)$, denotaremos por $\Gamma_n(A)$ o kernel da redução canônica $GL_n(A) \to GL_n(k)$. Se m_A é o ideal maximal de A é simples verificar que a multiplicação em $\mathrm{Ker}(GL_n(A/m_A^{r+1}) \to GL_n(A/m_A^r))$ resulta numa adição componente a componente, e portanto esse kernel é isomorfo ao produto de n^2 cópias do grupo aditivo de m_A^r/m_A^{r+1}, um k–espaço vetorial de dimensão finita, ou seja, é um p–grupo finito. Esse fato implica imediatamente que $\Gamma_n(A/m_A^r)$ é um p–grupo finito $(r = 1,2,\ldots)$. Como $\Gamma_n(A) = \varprojlim \Gamma_n(A/m_A^r)$, temos a

Proposição 1. Para cada A em $C(k)$, $\Gamma_n(A)$ é um pro–p–grupo.

Essa proposição tem uma conseqüência importante: se $\overline{\rho} : G \to GL_n(k)$ for uma representação residual (G e k fixados como sempre) e $\rho : G \to GL_n(A)$ for um homomorfismo que "levanta" $\overline{\rho}$ (A em $C(k)$), então ρ fatora-se por G/H onde H é o subgrupo de $\mathrm{Ker}\overline{\rho}$ tal que $\mathrm{Ker}\overline{\rho}/H$ é o maior pro–p–quociente de $\mathrm{Ker}\overline{\rho}$. De fato, não é difícil ver que H é um subgrupo normal de G e que temos a seguinte situação:



Como H é normal em G e $H \subseteq \mathrm{Ker}\overline{\rho}$ é tal que a restrição de ρ para $\mathrm{Ker}\overline{\rho}$ fatora-se por $\mathrm{Ker}\overline{\rho}/H$, $H \subseteq \mathrm{Ker}\rho$ e portanto ρ fatora-se por G/H.

Dizemos que esse quociente G/H é o *p–completamento de G relativo à $\overline{\rho}$.*

Relembramos que o *subgrupo de Frattini* $\Phi(G)$ de um grupo profinito G é a intersecção de todos os subgrupos abertos maximais de G. O *quociente de Frattini de* G é $G/\Phi(G)$. É útil definir também o *quociente de p–Frattini de* G como o maior quociente p–abeliano elementar de G. Um grupo profinito G é dito (topologicamente) finitamente gerado se for o fecho de um subgrupo finitamente gerado.

Proposição 2 (Burnside). Seja G um pro–p–grupo (topologicamente) finitamente gerado. Então $G/\Phi(G)$ é o maior quociente p–abeliano elementar de G e sua dimensão como $\mathbf{Z}/p\mathbf{Z}$–espaço vetorial é igual a $d(G)$, o número mínimo de elementos que geram G topologicamente. Além disso, se $x_1, \ldots, x_d \in G$ vão em geradores de $G/\Phi(G)$, então eles geram G.

Uma prova desse teorema pode ser vista em [Bo]. Veja também [Koch]. Daqui para frente, se G é um pro–p–grupo, o seu quociente de p–Frattini será denotado por $\overline{G}$.

Teorema 3 (Schur-Zassenhaus). Seja G um grupo profinito com um pro–p–subgrupo de Sylow P, normal em G, de índice finito e (topologicamente) finitamente gerado. Então G contém um subgrupo A projetando-se isomorficamente em G/P (e portanto

A tem ordem prima com p) e dois quaisquer subgrupos de G com essa propriedade são conjugados por um elemento de P (cf. [Ro]).

Assim, G é o produto semidireto de A e P o conhecimento de A, P e da ação $\phi : A \to \mathrm{Aut}(P)$ nos permite dar uma apresentação de G. Recordamos que, se P é um pro–p–grupo, $\mathrm{Aut}(P)$ denota o grupo dos isomorfismos bicontínuos de P e vale o teorema de P. Hall (cf. [Bo]) que afirma ser um pro–p–grupo o kernel da aplicação $\mathrm{Aut}(P) \to \mathrm{Aut}(\overline{P})$.

Usando esse resultado, não é difícil mostrar que para uma dada $\phi : A \to \mathrm{Aut}(\overline{P})$, só existe um produto semidireto (a menos de isomorfismo) de A e P. Tudo isso pode ser encontrado – com mais detalhes – na tese citada de N. Boston, assim como o seguinte teorema, que usaremos adiante:

Teorema 4. Na mesma situação do teorema 3 acima, se V for um subgrupo de $\overline{P}$ invariante sob a ação de A, existe um subgrupo fechado B de P, invariant sob a ação de A, gerado por $d(V) = \dim_{\mathbf{F}_p} V$ elementos, e projetando-se em V sob $P \to \overline{P}$ ($\mathbf{F}_p$ é o corpo finito com p–elementos).

Como exemplos significativos de aplicação desse teorema, daremos dois casos (cf. [Bo]) que aparecerão adiante:

(1) Suponhamos que a ação de A em V seja pela representação regular, isto é, existe um $\overline{x} \in V$ tal que

$V =< g.\overline{x};\ g \in A >$ e $d(V) = \#(A)$. Então se $x \in P$ vai em $\overline{x} \in \overline{P}$, posso tomar $B =< gx;\ g \in A >$.

(2) Suponhamos que V seja unidimensional gerado por $\overline{x}$ com a ação de A dada por $\phi : A \to \mathrm{Aut}(V) \cong \mathbf{F}_p^*$. Pelo teorema acima, existe $x \in P$ projetando-se em $\overline{x}$ tal que $B =< x >$ é A–invariante. A ação $\widetilde{\phi} : A \to \mathrm{Aut}(B)$ é dada pela composição de ϕ com o levantamento de Teichmüller $\mathbf{F}_p^* \hookrightarrow \mathbf{Z}_p^*$, ou seja,

x está em

$$E(\chi) = \{u \in P : g.u = u^{\chi(g)}.\forall\ g \in A\},$$

onde $\chi : A \to \mathbf{Z}_p^*$ é o carácter correspondente a ϕ, e a exponenciação acima é a operação usual de elevar um elemento de um pro–p–grupo a uma potência que é uma unidade p–ádica.

I-4 - Formas Modulares Ordinárias e Representações Ordinárias

Seja $f = \sum a_n q^n$ uma forma modular parabólica, de peso $\omega \geq 1$ em $\Gamma_1(N)$, com carácter $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ e que seja autoforma para os operadores de Hecke T_ℓ, com $\ell\ N_p$ (p um primo). Sem perda de generalidade, podemos supor que f seja normalizada e portanto $T_\ell f = a_\ell f$ e $U_p f = a_p f$. É bem conhecido que o corpo K_f gerado sobre $\mathbf{Q}$ pelos autovalores dos operadores de Hecke T_ℓ e U_p é uma extensão finita dos racionais, e o seu anel de inteiros $\mathcal{O}_f$ contém os coeficientes de Fourier de f.

Se λ for um primo de $\mathcal{O}_f$, denotamos por $\mathcal{O}_{f,\lambda}$ o completamento de $\mathcal{O}_f$ em λ e por $K_{f,\lambda}$ o completamento de K_f em λ. Se r for um primo, denotamos por Frob_r o automorfismo de Frobenius em r no grupo $\mathrm{Gal}(\overline{Q}/Q)$. Temos o resultado fundamental:

Teorema 5. Para cada primo λ de $\mathcal{O}_f$ existe uma representação contínua semisimples:

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(\mathcal{O}_{f,\lambda})$$

não ramificada fora de λ e dos primos que dividem N, e tal que se r for um primo que não divide N e $\lambda \cap \mathbf{Z}$, então:

$$\mathrm{tr}\rho_{f,\lambda}(\mathrm{Frob}_r) = a_r$$

$$\det\rho_{f,\lambda}(\mathrm{Frob}_r) = \varepsilon(r) r^{\omega-1}.$$

Esse teorema é devido a Eichler e Shimura (para $\omega = 2$) e Deligne (para $\omega \geq 2$) e a Deligne–Serre (para $\omega = 1$) (cf. [Schi], [De], [De-Se]).

Se tomarmos $N = p^n$, λ um primo sobre p e se denotarmos por k o corpo de restos de $\mathcal{O}_{f,\lambda}$, reduzindo a representação acima, $\rho_{f,\lambda}$, módulo o ideal maximal, obtemos

uma representação residual

$$\overline{\rho}_{f,\lambda} : G_{Q,S} \to GL_2(k),$$

onde $S = \{p, \infty\}$. Salvo menção contrária, no que se segue permaneceremos nessa situação particular que acabamos de descrever.

Seguindo Mazur, [Ma2], vamos considerar pares (f, λ) como acima, e fixar uma representação residual absolutamente irredutível e ordinária (para I = subgrupo de inércia em p)

$$\overline{\rho} : G_{Q,S} \to GL_2(k),$$

onde $S = \{p, \infty\}$. Diremos que f *é ordinária* (ou que o par (f, λ) é ordinário) se a_p for inversível em $\mathcal{O}_{f,\lambda}$ ou, equivalentemente, se $\overline{a_p}$ for não nulo em k. Diremos também que *o par* (f, λ) *pertence a* $\overline{\rho}$ se para todo primo $\ell \neq p$ tivermos:

$$\det(X - \overline{\rho}(\mathrm{Frob}_\ell)) \;=\; X^2 - \overline{a}_\ell X + \overline{\varepsilon(\ell)}.\ell^{\omega-1}.$$

Consideremos agora a representação

$$\rho_{f,\lambda} : G_{Q,S} \to GL_2(K_{f,\lambda})$$

cuja existência nos garante o teorema 5 acima, e no caso particular que nos interessa, isto é, $N = p^m$ e λ sobre p. Então sabemos que

$$\det(X - \rho_{f,\lambda}(\mathrm{Frob}_\ell)) \;=\; X^2 - a_\ell X + \varepsilon(\ell)\ell^{\omega-1}$$

e vale o seguinte teorema:

Teorema 6. Se (f, λ) é um par ordinário, então existe uma representação ordinária

$$\widetilde{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(\mathcal{O}_{f,\lambda})$$

não ramificada em nenhum primo (finito) diferente de p, equivalente sobre K_f a $\rho_{f,\lambda}$, e tal que a restrição a um grupo de decomposição em p, D_p é:

$$\widetilde{\rho}_{f,\lambda}\Big|_{D_p} \;=\; \begin{pmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix}$$

onde ε_1 é um carácter não ramificado.

Não é supérfluo observar que escolhemos trabalhar com Frobenius *geométrico* em vez do Frobenius *aritmético*, e portanto nossas representações não são as mesmas como por exemplo em [De]. O Frobenius aritmético é o usual, como no teorema 5 atrás, e o Frobenius geométrico é o seu inverso. Nós o preferimos para manter as mesmas notações de Mazur e de Wiles.

A prova pode ser encontrada em [M-W] ou, numa formulação mais geral, em [W]. Assim, *se* (f, λ) *for um par ordinário e pertencer a* $\overline{\rho}$, então existirá uma representação ordinária $\widetilde{\rho}_{f,\lambda}$ não ramificada fora de p, e que "levanta" $\overline{\rho}$, e portanto a classe de equivalência estrita (cf. I-1) de $\widetilde{\rho}_{f,\lambda}$ é univocamente determinada por um morfismo

$$h_{f,\lambda} : \mathbf{R}^0(G_{Q,S}, k, \overline{\rho}) \to \mathcal{O}_{f,\lambda}.$$

Fazemos de agora em diante a hipótese de que efetivamente *existe* um par ordinário pertencendo a $\overline{\rho}$. E vamos procurar construir um anel que "fatore" todos os $h_{f,\lambda}$, isto é, queremos um anel $\mathbf{T}^0(\overline{\rho})$ e um morfismo (em $C(k)$)

$$\mathbf{R}^0(\overline{\rho}) \to \mathbf{T}^0(\overline{\rho})$$

tal que se (f, λ) for um par ordinário pertencendo a $\overline{\rho}$ então existirá $\eta_{f,\lambda} : \mathbf{T}^0(\overline{\rho}) \to \mathcal{O}_{f,\lambda}$ tal que o diagrama comute:

$$\begin{array}{ccc} \mathbf{R}^0 & \xrightarrow{h_{f,\lambda}} & \mathcal{O}_{f,\lambda} \\ & \searrow \quad \nearrow \eta_{f,\lambda} & \\ & \mathbf{T}^0 & \end{array}$$

Se existir um tal anel $\mathbf{T}^0(\overline{\rho})$, ele será então universal para representações ordinárias provenientes de formas modulares ordinárias. Vamos agora esboçar a construção de $\mathbf{T}^0(\overline{\rho})$. Seja $\mathcal{H}$ a álgebra polinomial comutativa sobre Λ (cf. I-1) gerada pelos símbolos T_ℓ, $\ell \neq p$, e U_p.

$$\mathcal{H} = \Lambda[U_p, \ldots, T_\ell, \ldots \ (\ell \neq p)].$$

Para cada par (f, λ) pertencendo a $\overline{\rho}$, consideremos o homomorfismo de Λ–álgebras

$$\varphi(f, \lambda) : \mathcal{H} \to \mathcal{O}_{f,\lambda}$$

que leva T_ℓ em a_ℓ e U_p em a_p. Consideremos o ideal

$$I_w = \bigcap \mathrm{Ker}\varphi(f, \lambda)$$

onde a intersecção é tomada sobre todos os pares (f, λ) ordinários que pertencem a $\overline{\rho}$, tais que f tem peso w.

Teorema 7 (Hida). Se $w \geq 2$ o ideal I_w independe de w.

A álgebra quociente $\mathcal{H}/I_w$ será chamada álgebra de Hecke de Hida, e denotada $\mathbf{T}^0(\overline{\rho})$. Por construção obtivemos um homomorfismo $\mathbf{R}^0(\overline{\rho}) \to \mathbf{T}^0(\overline{\rho})$ que "fatora" todos os $h_{f,\lambda}$, onde (f, λ) é um par ordinário pertencendo à $\overline{\rho}$ e f tem peso $w \geq 2$.

Essa teoria é devida a Hida e pode ser vista em [H1], [H2], ou no artigo expositório [T]. Veja também [Gou1]. Podemos agora enunciar a seguinte conjectura de Mazur:

conjectura: O homomorfismo $\mathbf{R}^0 \to \mathbf{T}^0$ é um isomorfismo.

Em [Ma 1], Mazur provou essa conjectura para uma classe muito particular de representações, as "representações diedrais especiais". Um pouco mais a respeito pode ser encontrado em [M-T]. A conjectura implica que toda representação ordinária de $\mathrm{Gal}(\overline{Q}/Q)$ em $GL_2(\mathcal{O})$, não ramificada fora de p, onde $\mathcal{O}$ é um anel de valorização discreta de posto finito sobre $\mathbf{Z}_p$, que for um levantamento de $\overline{\rho}$, de fato está associada a uma forma modular (p–ádica) ordinária cujos coeficientes de Fourier estão em $\mathcal{O}$.

Conjectura-se também que o anel universal das deformações de $\overline{\rho}$, $\mathbf{R}(\overline{\rho})$ seja isomorfo a uma álgebra de Hecke mais geral $\mathbf{T}$ (veja [Gou] para definições e propriedades). Espera-se que $\mathbf{T}$ seja uma álgebra de séries formais em três variáveis sobre $W(k)$ e sabe-se que $\mathbf{T}^0$ é uma extensão finita e plana de uma álgebra de séries formais em uma variável sobre $W(k)$ (cf. [H1], [H2]).

Assim, combinando tais conjecturas – bem como os casos particulares conhecidos, obtemos uma relação (conjectural) entre $\mathbf{R}$ e $\mathbf{R}^0$, a saber: o morfismo canônico $\mathbf{R} \to \mathbf{R}^0$ teria que ser sobrejetor e $\dim \text{Krull } \mathbf{R} = \dim \text{Krull } \mathbf{R}^0 + 2$.

No capítulo III, provaremos a sobrejeção acima, e se $\overline{\rho}$ for moderadamente ramificada, mostraremos que

$$\dim \text{Krull } \mathbf{R} \geq \dim \text{Krull } \mathbf{R}^0 + 2.$$

CAPÍTULO II

DEFORMAÇÕES ORDINÁRIAS DE REPRESENTAÇÕES NÃO RAMIFICADAS EM p

Neste capítulo consideramos deformações de representações residuais $\overline{\rho}$ que não são ramificadas em p. Ou seja, pensamos em

$$\overline{\rho} : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(k),$$

onde k é um corpo finito de característica p, que não ramifica em p. Naturalmente, $\overline{\rho}$ vai ramificar nalgum outro primo ℓ, e podemos então considerar deformações que não ramificam fora de $S = \{p, \ell, \infty\}$. Tais representações residuais aparecem, por exemplo, associadas a formas modulares de peso $w = 1$ em $\Gamma_1(N)$, onde N é um primo distinto de p, via o teorema de Deligne (Deligne–Serre, para $w = 1$), que enunciamos como o teorema 5 de I-4. Nesse caso, se considerarmos o functor $F^0 : C(k) \to$ Conjuntos, dado por

$$F^0(A) = \{\text{deformações ordinárias de } \overline{\rho} \text{ para } A\}$$

Teremos que $F^0(k) = \emptyset$, pois $\overline{\rho}$ não ramifica em p, e portanto não pode ser ordinária em p. Vamos analisar essa situação em alguns casos especiais em que $\overline{\rho}(\mathrm{Gal}(\overline{Q}/Q)) \cong S_3$, o grupo diedral de ordem 6, na direção da pergunta mais geral:

> *"(...) and it would be very interesting to understand this situation better. For example, will the locus of ordinary deformations in* $X = \mathrm{Spec}(\mathbf{R})$ *be a subscheme?"* [Gou2])

II-1 - A Situação Geral

Consideremos um número primo p e um fecho algébrico $\overline{Q}_p$ dos racionais p–ádicos Q_p. Denotemos por $\overline{Q}$ o fecho algébrico de Q contido em $\overline{Q}_p$, que nos dá um morfismo injetor

$$(*) \qquad G_{Q_p} \hookrightarrow G_Q$$

(recordamos que se F é um corpo, G_F denota $\mathrm{Gal}(\overline{F}/F)$).

Se tivermos uma representação residual

$$\overline{\rho} : G_Q \to GL_2(\mathbf{F}_p)$$

denotaremos por $\overline{\rho}_p$ a composta de $\overline{\rho}$ com $(*)$ acima, ou seja, obtemos uma representação local:

$$\overline{\rho}_p : G_{Q_p} \to GL_2(\mathbf{F}_p).$$

Denotaremos por N e N_p os kernéis de $\overline{\rho}$ e $\overline{\rho}_p$ respectivamente e por L e L_p os corpos fixos por N e N_p, ou seja, os corpos de decomposição de ρ e $\overline{\rho}_p$ respectivamente. Seja S um conjunto finito de primos de L, contendo os primos sobre p, e indiquemos por L_v o completamento de L num $v \in S$. Pela nossa escolha inicial, temos que $L_{v_1} = L_p$ para certo v_1.

Já vimos em I-3 (e recordamos aqui) que se $H \subset N$ é o subgrupo característico fechado tal que $P := N/H$ é o grupo de Galois da maior pro–p–extensão de L em $\overline{Q}$ que é não ramificada fora de S (ramificação no infinito sendo permitida), então H é normal em G_Q e $G := G_Q/H$ é chamado o p–completamento de G_Q relativo a $\overline{\rho}$. Analogamente consideramos o subgrupo $H_p \subset N_p$ tal que $P_p = N_p/H_p$ é o maior pro–p–quociente de N_p e o p–completamento $G_p = G_{Q_p}/H_p$ de G_{Q_p} relativo a $\overline{\rho}_p$.

Em I-3 observamos que se A é um anel local Noetheriano completo cujo corpo de restos é $\mathbf{F}_p$, então todo levantamento $\rho : G_Q \to GL_2(A)$ de $\overline{\rho}$ se fatora por G, pois $\mathrm{Ker}(GL_2(A) \to GL_2(\mathbf{F}_p))$ é um pro–p–grupo.

Assim, por construção temos o seguinte diagrama de grupos profinitos, cujas linhas horizontais são exatas:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P & \longrightarrow & G & \longrightarrow & A & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & P_p & \longrightarrow & G_p & \longrightarrow & A_p & \longrightarrow & 1 \end{array}$$

Aqui $A \cong \mathrm{Im}(\overline{\rho})$ e $A_p \cong \mathrm{Im}(\overline{\rho}_p)$ em $GL_2(\mathbf{F}_p)$.

Da teoria local e global de Corpos de Classes, sabemos que os quocientes de p–Frattini, $\overline{P}_p$ e $\overline{P}$ são finitos, e portanto, pela proposição 2 de I-3, P_p e P são (topologicamente) finitamente gerados.

Em todo este capítulo suporemos que A_p tem ordem prima com p. Já sabemos da teoria local dos corpos de classes que temos um isomorfismo de $\mathbf{F}_p[A_p]$–módulos

$$L_p^*/(L_p^*)^p \cong \overline{P}_p$$

e que

$$\overline{P}_p = \mathbf{F}_p[A_p] \oplus \boldsymbol{\mu}_p(L_p) \oplus \mathbf{F}_p$$

onde $\mathbf{F}_p[A_p] \oplus \boldsymbol{\mu}_p(L_p)$ é a imagem do subgrupo de inércia de P_p em $\overline{P}_p$ e a ação de A_p na componente $\mathbf{F}_p$ é a ação trivial (veja o lema 1 do Capítulo III).

Seja E o grupo das unidades (globais) do anel de inteiros de L e se v for um primo não arquimediano, pomos E_v para o grupo das unidades (locais) do anel de L_v. Como podemos ver no Capítulo III, a transformação de Artin global $\psi_L : I_L \to \mathrm{Gal}(L^{ab}/L)$ induz um morfismo A–equivariante nos p–Frattinis

$$\oplus_{v \in S} \overline{E}_v \to \overline{P},$$

cujo kernel contém a imagem de $\overline{E}$, o p–Frattini do grupo das unidades globais.

Definição: *([Ma1])*. O par (L, S) é chamado *neat** para p se

* Preferimos manter aqui a terminologia original de Mazur.

(a) A aplicação $\overline{E} \to \oplus_{v \in S} \overline{E}_v$ for injetora, isto é, se uma unidade global for localmente uma potência p–ésima (para todo $v \in S$) então ela será (globalmente) uma potência p–ésima.

(b) O morfismo $\oplus_{v \in S} \overline{E}_v \to \overline{P}$ é sobrejetor, ou seja, o número de classes de L é primo com p.

(c) A aplicação $\mu_p(L) \to \oplus_{v \in S} \mu_p(L_v)$ é sobrejetora.

É claro que se (L, S) for *neat* para p, temos a seqüência exata:

$$0 \longrightarrow \overline{E} \longrightarrow \oplus_{v \in S} \overline{E}_v \longrightarrow \overline{P} \longrightarrow 0$$

Proposição 1. Se A_p for primo com p e (L, S) for *neat* para p então

(a) Se L for totalmente real $\overline{P} \cong \mathbf{F}_p$ (A–ação trivial).

(b) Se L for totalmente complexo, teremos $\overline{P} \cong \mathrm{Ind}_C^A \widetilde{\mathbf{F}}_p \oplus \mathbf{F}_p$

onde $C \subset A$ é o subgrupo gerado pela imagem de uma conjugação complexa e $\widetilde{\mathbf{F}}_p$ é a representação unidimensional de $\mathbf{F}_p[\mathbf{C}]$ com ação não trivial de $\mathbf{C}$.

Prova. Veja [Bo-Ma].

Se H for um pro–p–grupo, o posto de geradores será denotado $d(H)$ e o posto de relações será denotado $r(H)$ (veja [Koch], §6). Se F for um corpo, seja $\delta(F) = 1$ se F contiver uma raiz p–ésima não trivial de 1 e $\delta(F) = 0$ caso contrário.

Proposição 2 ([Koch], Satz 10.3, Satz 11.8).

(a) $r(P_p) = \delta(L_p)$

(b) $d(P_p) = [L_p.Q_p] + 1 + \delta(L_p)$

(c) $r(P) = (\sum_{v \in S} \delta(L_v)) - \delta(L) + \dim B_S$

(d) $d(P) = r_2 + 1 + r(P)$

onde $B_S = \{x \in L^* : (x) = I^p \text{ e } x \in (L_v^*)^p \ \forall\, v \in S\}/(L^*)^p$ é o grupo que aparece no Capítulo III e r_2 é o número de imersões complexas de L.

Observação. Da definição, sai que se (L, S) for *neat* para p, então $B_S = (0)$. Decorre da proposição acima que P é um pro–p–grupo livre se e só se $B_S = (0)$ e o morfismo $\mu_p(L) \to \oplus_{v \in S} \mu_p(L_v)$ for sobrejetor. Assim, se (L, S) for *neat* para p, então P será um pro–p–grupo livre.

II-2 - Uma Classe Especial de Representações

Neste parágrafo, introduziremos uma classe especial de representações residuais $\overline{\rho}: G_{Q,S} \to GL_2(k)$, onde $S = \{\ell, p, \infty\}$, k tem característica p, que é não ramificada em p, onde poderemos dizer alguma coisa sobre as deformações universais e as deformações ordinárias.

Seja K_1/Q uma extensão cúbica não Galoisiana com discrimante $-\ell$, onde ℓ é um primo ≥ 5 verificando a congruência $-\ell \equiv 1 \bmod 4$. Consideremos a extensão L/Q, onde L é o fecho Galoisiano de K_1. Então L contém o corpo quadrático $Q(\sqrt{-p})$ e $\mathrm{Gal}(L/Q) \cong S_3$ (o grupo simétrico em 3 letras). Para construirmos a nossa classe especial de representações, tomamos o conjunto de primos $S = \{\ell, p, \infty\}$, com $\ell \neq p$, e

$$\overline{\rho}: G_{Q,S} \to GL_2(k)$$

uma representação obtida da composição da projeção canônica $G_{Q,S} \twoheadrightarrow \mathrm{Gal}(L/Q)$ com uma inclusão $\mathrm{Gal}(L/Q) \hookrightarrow GL_2(k)$, para um corpo k finito, de característica p.

Vamos analisar as condições sob as quais o par (L, S) é *neat* para p. Mantendo as notações de II-1, precisamos considerar os seguintes grupos:

(1) $\mathrm{Ker}(E/E^p \to \oplus_{v \in S} E_v/E_v^p)$

(2) $\mathrm{Coker}(\oplus_{v \in S} E_v/E_v^p \to \overline{P})$

(3) $\mathrm{Coker}(\mu_p(L) \to \oplus_{v \in S} \mu_p(L_v))$

onde os primos de S acima são somente os não arquimedianos. Precisamos verificar quando esses três grupos são triviais. A terceira condição é simples: se $v \in S$, não

arquimediano, então L_v conterá uma raiz p–ésima primitiva de 1 só se Q_p ou Q_ℓ (no caso de v estar sobre p ou sobre ℓ) a contiver; assim, no caso em que v está sobre p, temos $\mu_p(L_v) = 0$, e no caso em que v está sobre ℓ, isso só será possível se $p \nmid (\ell - 1)$. Temos então a conclusão que se $p \nmid (\ell - 1)$, então o grupo em (3) é trivial. Para que o grupo em (2) seja trivial, já vimos que p não pode dividir o número de classes de L, e portanto essa condição será assumida como hipótese.

Resta considerar a seqüência

$$0 \longrightarrow E/E^p \longrightarrow \oplus_{v|p} E_v/E_v^p \oplus_{w|\ell} E_w/E_w^p,$$

que queremos que seja exata. Observamos inicialmente (cf. [Neu], prop.1.5, Chap.III, §2), que se $w \mid \ell$

$$(L_w^* : L_w^{*p}) = p.(E_w : E_w^p) = \frac{p}{|p|_\ell}.\#\mu_p(L_w)$$

onde $|p|_\ell$ denota a valorização ℓ–ádica do primo p. Como $\#\mu_p(L_w) = 1$, segue que $(E_w : E_w^p) = 1$, ou seja, basta considerarmos a exatidão de

$$0 \longrightarrow E/E^p \longrightarrow \oplus_{v|p} E_v/E_v^p$$

Vamos exibir seguindo Mazur uma família de extensões L/Q, com grupo de Galois S_3, discriminante–ℓ, uma família de primos p tais que a seqüência acima seja exata. Inicialmente, observe-se que como o discriminante é negativo, L é um corpo totalmente complexo e conseqüentemente a representação de G no Q–espaço vetorial $E \otimes Q$ é a representação bidimensional irredutível (cf. [Ma1]). Portanto, se a imersão natural $E \to \oplus_{v|p} E_v$ não tiver a propriedade de que toda a imagem esteja contida no subgrupo das potências p–ésimas, então o grupo em (1) se anulará, e a seqüência anterior será exata.

Consideremos os polinômios $f(X) = X^3 + aX + 1$ para inteiros a tais que $27 + 4a^3$ seja um número primo ℓ.

Definição. Um corpo cúbico especial (de discriminante $-\ell$) é um corpo $K_1 = Q(x)$, onde x é uma raiz de $f(X) = 0$.

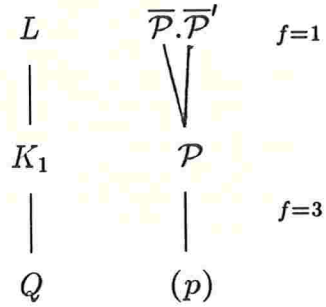
De fato, K_1 tem discriminante $-\ell$, e pode-se mostrar (veja-se referência em [Ma1]) que o grupo de unidades de K_1 é gerado por $\pm x$. Seguem-se alguns exemplos de ℓ tais que $-\ell$ é o discriminante de uma cúbica especial: 23, 31, 59, 283, 1399, 4027, 5351, 11003, 16411, 32027, 97583, 119191, 157243, 202639.

Seja K_1 uma cúbica especial de discriminante $-p$ e L o fecho galoisiano de K_1 sobre Q, isto é, um corpo de decomposição de $f(X)$ sobre Q, contendo x. É claro que x é uma unidade em $\mathcal{O}_1$, o anel de inteiros de K_1.

Para um primo $p \neq \ell$, temos as seguintes possibilidades:

(I) $-\ell$ é resíduo quadrático mod p. Há dois casos:

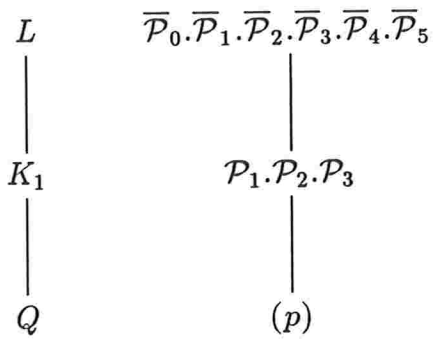
(I.1)



$[L_{\overline{\mathcal{P}}} : Q_p] = 3$

p inerte na cúbica $X^3 + aX + 1$ irredutível mod p.

(I.2)

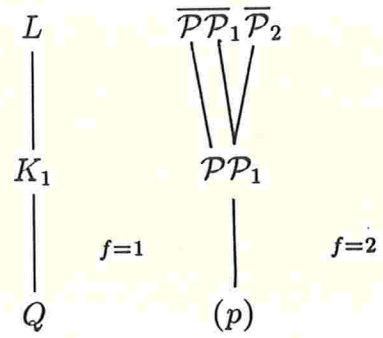


$[L_{\overline{\mathcal{P}}_i} : Q_p] = 1$

(p) se decompõe totalmente.

$X^3 + aX + 1$ fatora-se totalmente.

(II) $-\ell$ não é resíduo quadrático mod p:



$[L_{\overline{\mathcal{P}}} : Q_p] = 2$

$X^3 + aX + 1 \equiv (X - \alpha)(X^2 + bX + c) \mod p.$

Trataremos esses casos separadamente. *Iniciamos com o caso* I-1, isto é, p inerte na cúbica. Precisaremos do

Lema 1. Seja K uma extensão finita de Q e $\alpha \in K^*$. Seja p um número primo e ζ uma raiz p–ésima primitiva de 1. Se $\alpha = \beta^p$ para certo $\beta \in K(\zeta)$, então $\alpha = \delta^p$ para certo $\delta \in K^*$.

Prova. Como $\beta \in K(\zeta)$ e $[K(\zeta) : K]$ divide $(p-1)$, se pusermos $m = [K(\beta) : K]$, teremos que $m \mid (p-1)$, ou seja, m e p serão relativamente primos. Podemos então conseguir x e y em $\mathbf{Z}$ tais que $1 = mx + py$. Seja $N = N_{K(\beta)/K}$ a norma, da extensão $K(\beta)$ para K. Pondo $\gamma = N(\beta)$ e salientando que $\alpha \in K^*$, $\alpha = \beta^p$, vem

$$\alpha^m = N(\alpha) = N(\beta^p) = N(\beta)^p = \gamma^p.$$

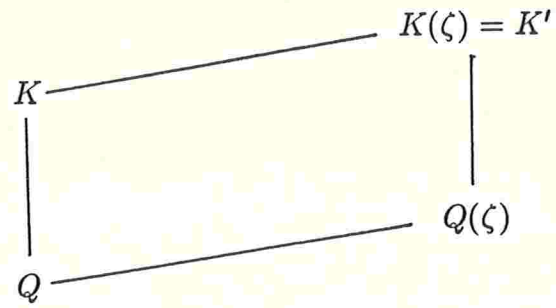
E portanto

$$\alpha = \alpha^{mx+py} = (\gamma^x.\alpha^y)^p.$$

Pondo $\delta = \gamma^x.\alpha^y$, temos que $\delta \in K$ e $\alpha = \delta^p$.

C.Q.D.

Utilizando o lema na seguinte situação $K = K_1 = Q(x)$, uma cúbica especial, vemos que x será uma potência p–ésima em K se e só se for uma potência p–ésima em $K(\zeta)$. No diagrama abaixo,



como p é inerte em K e ramifica totalmente em $Q(\zeta)$, o único primo de $K(\zeta)$ sobre p é $(1-\zeta)$. Além disso, é claro que $K(\zeta)$ é totalmente complexo. Seja P' o grupo de Galois da maior pro–p–extensão de $K(\zeta) = K'$ não ramificada fora de $S' = \{p\}$. Temos o

Teorema (Brumer, [Bru]). Na situação acima, são equivalentes:

(1) P' é livre pro–p

(2) K' é totalmente imaginário, existe um único primo P de K' sobre p, e o subgrupo gerado pela classe de P contém a componente p–primária do grupo de classes de ideais de K'.

No nosso caso, $P = \{(1-\zeta)\}$ é um ideal principal, donde P' será um pro–p–grupo livre se e só se p não dividir o número de classes de $K' = K(\zeta)$. Então, supondo que p $h(K')$, como K' e K'_P contêm as raízes p–ésimas de 1, e $S' = \{p\}$, temos que $B_{S'} = (0)$, donde $(0) = B_{S'} \cong \mathrm{Ker}(E'/E'^p \to E_P/E_P^p)$, onde E' é o grupo de unidades de E' e E_P é o grupo de unidades locais de K'_P.

Como x não é potência p–ésima K, pelo lema 1, não é potência p–ésima em K', e portanto, pela injetividade de $E'/E'^p \to E_P/E_P^p$, não é potência p–ésima em E'_P. Como $L_{\overline{\mathcal{P}}} = (K_1)_{\mathcal{P}} \subset K'_{\mathcal{P}}$, x não pode ser potência p–ésima em E_v, para v/p. Pelo comentário que fizemos no fim da página [25], como encontramos um elemento x nas

condições acima, segue que

$$0 \to E/E^p \to \oplus_{v|p} E_v/E_v^p$$

tem que ser exata. Assim, neste caso em que $-\ell$ é resíduo quadrático módulo p e p é inerte na cúbica, provamos que se p não dividir o número de classes de $K(\zeta)$, então a seqüência exata acima tem que ser exata.

Consideremos agora o **caso I-2**, isto é, p se decompõe totalmente. Neste caso, $X^3 + aX + 1 \equiv (X - r_1)(X - r_2)(X - r_3) \mathrm{mod} p$. Seja $m \in \mathbf{Z}$ tal que sua redução mod p seja r_1. Então $N_{K_1/Q}(x - m) = m^3 - am - 1 = \alpha p^\nu$, onde $\nu \geq 1$ e $p \nmid \alpha$. Se $\nu = 1$, defino $\pi = x - m$. Vamos mostrar que no localizado a imagem de π é um uniformizante local

$$N_{H/Q}(\pi) = N_{K_1/Q}(\pi)^2 = \alpha^2 p^2.$$

Se denotarmos por $v_{\mathcal{P}_i'}$, $i = 0, 1, \ldots$ as valorizações associadas aos primos $\mathcal{P}_i'$ sobre p, teremos:

$$v_{\mathcal{P}_0'}(N_{H/Q}(\pi)) = \sum_{\sigma \in S_3} v_{\mathcal{P}_0'}(\sigma\, \pi)$$

e como p não ramifica, a restrição de $v_{\mathcal{P}_0'}$ a Q é v_Q, a valorização p–ádica usual de Q e portanto:

$$2 = \sum_{i=0}^{5} v_{\mathcal{P}_i'}(\pi).$$

Da Teoria de Kummer, sabemos que $\mathcal{P}_1$ (na cúbica K_1) é gerado por (p, π), donde, como $\mathcal{P}_0'$ e $\mathcal{P}_1'$ são os únicos ideais acima de $\mathcal{P}_1$,

$$2 = v_{\mathcal{P}_0'}(\pi) + v_{\mathcal{P}_1'}(\pi)$$

Como $\pi \in K_1 = Q(x)$, $v_{\mathcal{P}_0'}(\pi) = v_{\mathcal{P}_1'}(\pi)$, donde $v_{\mathcal{P}_0'}(\pi) = 1$.

Se $\nu \geq 2$, $N_{K_1/Q}(x - (m + p)) = (m + p)^3 - a(m + p) - 1 =$

$= m^3 + 3m^2 p + 3mp^2 + p^3 - am - ap - 1$

$= (3m^2 - a)p + 3mp^2 + p^3 \mod p^\nu.$

Como $(3m^2 - a) = f'(m)$ e $f(m) \equiv 0 \mod p$, pela separabilidade do polinômio $f(X) \pmod p$, segue que $p \nmid (3m^2 - a)$. Pondo $\pi = x - (m + p)$, a mesma conta anterior mostra que a imagem de π no localizado tem que ser um uniformizante, e portanto a seqüência da página [25] é exata.

Para o **caso II**, onde $f(X) = (X - r)(X^2 + bX + c) \mod p$, o mesmo truque acima mostra que posso tomar $\pi = x - m$ (ou $\pi = x - m - p$ se necessário), onde $m \equiv r \mod p$, de modo que $v_{\overline{P}}(\pi) = 1$.

Denotando por Π a imagem de π no completado, vamos mostrar agora que a imagem de x nos completados, dada por $x = (\text{inteiro}) + \Pi$ não pode ser uma potência p–ésima. De fato, mostrarmos que nenhuma potência p–ésima pode ser escrita como (inteira) + Π(unidade):

Se $y = a_0 + a_1\Pi$, $a_0 \in \mathbf{Z}_p^{\times}$, y unidade, então

$$y^p = a_0^p + \left[p\, a_0^{p-1} a_1 + \binom{p}{2} a_0^{p-2} a_1^2 \Pi + \ldots + a_1^p \Pi^{p-1} \right] \Pi$$

e portanto, como $\Pi \mid p$, Π divide a expressão entre colchetes, donde $y^p - a_0^p = 0 \pmod{\Pi^2}$. Se $y^p = n + u\Pi$, com n inteiro e u uma unidade, então $n \equiv a_0^p \pmod \Pi$ e portanto $y^p - a_0^p \equiv u\Pi \pmod \Pi$, donde $u\Pi \equiv 0 \pmod{\Pi^2}$, o que é impossível, pois u é unidade.

Ou seja, encontramos um elemento inversível x que não é potência p–ésima no completado de L (que é igual ao completado de K_1) nos casos I-2 e II.

Definição. Uma representação $\overline{\rho} : G_{Q,\{\ell,p,\infty\}} \to GL_2(\mathbf{F}_p)$ é dita uma representação especial se for uma representação residual construída como no início de II-2, a partir de uma cúbica especial K_1/Q, onde $K_1 = Q(x)$ e $x^3 + ax + 1 = 0$ com $\ell = 27 + 4a^3$.

Sumarizamos agora tudo o que fizemos com o

Teorema 1. Seja $\overline{\rho} : G_{Q,\{\ell,p,\infty\}} \to GL_2(\mathbf{F}_p)$ uma representação especial e L/Q o seu corpo de decomposição. Então se $p \nmid (\ell - 1)$ e p não dividir o número de classes de $L(\zeta)$,

onde ζ é uma raiz p–ésima primitiva da unidade, então o grupo de Galois P da maior pro–p–extensão de L não ramificada fora de $\{\ell, p, \infty\}$ é livre em 4 geradores.

Prova: A única coisa que falta é mostrar que a condição $p \nmid h(L(\zeta))$ implica $p \nmid h(L)$ e $p \nmid h(K_1(\zeta))$, que eram as condições que obtivemos. Como $p \nmid [L(\zeta) : L]$ e $p \nmid [L(\zeta) : K_1(\zeta)]$, isso é imediato (cf. [Wa]).

C.Q.D.

III-3 - Deformação Universal de Representações Especiais

Neste parágrafo, vamos calcular explicitamente o espaço universal das deformações de $\overline{\rho}$ (onde $\overline{\rho}$ é uma representação especial, do §2) e a deformação universal ρ^u, e preparar o caminho para uma análise mais detalhada do espaço universal $X = \mathrm{Spec}(\mathbf{R}(\overline{\rho}))$. Começamos com um fato absolutamente geral: se $\overline{\rho} : G_{Q,S} \to GL_2(\mathbf{F}_p)$ for uma representação residual com corpo de decomposição L e P for o grupo de Galois da maior pro–p–extensão de L não ramificada fora de S, com $A = \mathrm{Im}(\overline{\rho})$ de ordem prima com p, então temos a

Proposição 1. Se P for livre pro–p, então o anel versal (veja o Teorema 1 do Capítulo I, §1) de deformações de $\overline{\rho}$ é $\mathbf{R}(\overline{\rho}) = \mathbf{Z}_p[[T_1, \ldots, T_r]]$, onde $r = \dim_{\mathbf{F}_p} \mathrm{Hom}_A(\overline{P}, \Gamma_2(\mathbf{F}_p[\varepsilon]))$ e $\mathrm{Hom}_A(\overline{P}, \Gamma_2(\mathbf{F}_p[\varepsilon]))$ é o grupo dos morfismos A–equivariantes do Frattini $\overline{P}$ em $\Gamma_2(\mathbf{F}_p[\varepsilon])$, onde $\mathbf{F}_p[\varepsilon]$ é o anel dos números duais de $\mathbf{F}_p$ (cf. Capítulo III, no fim do lema 2).

Prova: Se B for um anel de $C(\mathbf{F}_p)$ com ideal maximal m, a obstrução ao levantamento de uma representação $\rho : G_{Q,S} \to GL_2(B/m^s)$ para B/m^{s+1} está em $H^2(G_{Q,S}M)$, onde $M = \mathrm{Ker}(GL_2(B/m^{s+1}) \to GL_2(B/m^s))$. Isso pode ser visto se considerarmos o produto fibrado de ρ e π, como abaixo:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & G_{Q,S} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & M & \longrightarrow & GL_2(B/m^{s+1}) & \xrightarrow{\pi} & GL_2(B/m^s) & \longrightarrow & 1 \end{array}$$

Assim, se esse nosso elemento de $H^2(G_{Q,S}, M)$ for trivial, isto é, se a seqüência exata de cima cindir, isso me dará um morfismo $\rho' : G_{Q,S} \to GL_2(B/m^{s+1})$ levantando ρ. Já sabemos que M é um grupo abeliano finito p–elementar (cf. I-3, antes da prop.1). Com as nossas hipóteses, é fácil ver que $H^2(G_{Q,S}, M) = 0$. De fato, como P é livre pro–p, $H^2(P, M) = 0$ e como $G_{Q,S}/P$ tem ordem prima com p, a restrição res: $H^2(G_{Q,S}, M) \to H^2(P, M)$ é injetora. Ou seja, qualquer B em $C(\mathbf{F}_p)$ tem a propriedade de que existe pelo menos um morfismo de $\mathbf{R}(\overline{\rho})$ para B.

Como vimos no §1 do Capítulo I, todo anel B de $C(\mathbf{F}_p)$ é um quociente de $\mathbf{Z}_p[[T_1, \ldots, T_r]]$ onde $r = \dim_{\mathbf{F}_p} t_B^*$, e portanto $\mathbf{R}(\overline{\rho})$ tem que ser um anel de séries formais de potências $\mathbf{R}(\overline{\rho}) = \mathbf{Z}_p[[T_1, \ldots, T_r]]$.

C.Q.D.

Observações: (1) O grupo $G_{Q,S}$ do teorema anterior na verdade deve ser substituído pelo seu p–completamento relativo a $\overline{\rho}$, e a prova é a mesma.

(2) O fato de que o número de variáveis r é o do enunciado pode ser visto em [Bo]. Esse número é o produto interno das representações $\overline{\phi} : A \to \mathrm{Aut}(\overline{P})$ e $\mathrm{Ad}(\overline{\rho})$, a representação adjunta de $\overline{\rho}$.

(3) No caso das nossas representações especiais, veremos adiante que $\mathbf{R}(\overline{\rho}) = \mathbf{Z}_p[[T_1, T_2, T_3]]$.

A menos de equivalência, temos 3 representações irredutíveis de $A \cong S_3$ sobre $\mathbf{F}_p$:

1 = a representação trivial

ϵ = a representação sinal

χ = a representação bidimensional irredutível.

Proposição 2. Se L/Q for o corpo de decomposição de uma representação residual $\overline{\rho}$

associada ao corpo cúbico especial K_1, então:

(a) Se p for inerte em K_1 (isto é, o caso I-1), então existe uma $\mathbf{F}_p$–base de $\overline{P}_p$ consistindo de $\overline{\xi}$, $\overline{\eta}$, $\overline{\varphi}$, $\overline{\psi}$ tal que $\overline{\xi}$, $\overline{\eta}$, $\overline{\varphi}$ geram a imagem da inércia em $\overline{P}_p$ e a ação de τ, o gerador de $A_p = \mathrm{Im}(\overline{\rho}_p)$, é dada por

$$\tau.\overline{\xi} = \overline{\xi}, \quad \tau\overline{\eta} = \overline{\varphi}, \quad \tau\overline{\varphi} = -\overline{\eta} - \overline{\varphi}, \quad \tau.\overline{\psi} = \overline{\psi}.$$

(b) Se p se decompor totalmente em L, (o caso I-2), então existe uma $\mathbf{F}_p$–base de $\overline{P}_p$ consistindo de $\overline{\xi}$, $\overline{\eta}$, onde $\overline{\xi}$ é a imagem da inércia em $\overline{P}_p$. (Neste caso, $A_p = \{1\}$).

(c) Se $-\ell$ não for resíduo quadrático mod p (o caso II), então existe uma $\mathbf{F}_p$–base de $\overline{P}_p$ consistindo de $\overline{\xi}$, $\overline{\eta}$, $\overline{\varphi}$, onde $\overline{\xi}$ e $\overline{\eta}$ geram a imagem da inércia em $\overline{P}_p$ e a ação de σ, o gerador de $A_p = \mathrm{Im}(\overline{P}_p)$ é dada por $\sigma\overline{\xi} = \overline{\xi}$, $\sigma\overline{\eta} = -\overline{\eta}$, $\sigma\overline{\varphi} = \overline{\varphi}$.

Prova: (a) Neste caso, $A_p = \{1, \tau, \tau^2\}$ e já vimos no início do §1 deste Capítulo que a imagem da inércia em $\overline{P}_p$ é isomorfa à $\mathbf{F}_p[A_p]$ (pois L_p não contém as raízes p–ésimas da unidade). Assim, usando a forma racional de τ,

$$\tau \approx \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

escolho, por exemplo: $\overline{\xi} = 1 + \tau + \tau^2$, $\overline{\eta} = \tau - \tau^2$, $\overline{\varphi} = \tau^2 - 1$. Como $\overline{P}_p = \mathbf{F}_p[A_p] \oplus \mathbf{F}_p$, com ação trivial de A_p em $\mathbf{F}_p$, escolho $\overline{\varphi}$ um gerador de $\mathbf{F}_p$, e temos aí a parte (a).

(b) Neste caso, $A_p = \{1\}$, $\overline{P}_p = \mathbf{F}_p \oplus \mathbf{F}_p$ e $\mathbf{F}_p = \mathbf{F}_p[A_p]$ é a imagem da inércia. O resultado é claro.

(c) Agora, $A_p = \{1, \sigma\}$, onde $\sigma^2 = 1$, $\overline{P}_p = \mathbf{F}_p[A_p] \oplus \mathbf{F}_p$, tomo $\overline{\xi} = 1 + \sigma$, $\overline{\eta} = 1 - \sigma$, $\overline{\varphi}$ um gerador de $\mathbf{F}_p$.

C.Q.D.

Proposição 3. O quociente de Frattini $\overline{P}$ é 4–dimensional e a ação natural de $A \cong S_3$ em $\overline{P}$ é equivalente à

$$1 \oplus \epsilon \oplus \chi$$

Prova: Já sabemos que $p \nmid |A_p|$ e no teorema 1 acima provamos que (L, S) é *neat* para p, donde, pela parte (b) da proposição 1 do §2 deste capítulo,

$$\overline{P} \simeq \mathrm{Ind}_C^A \widetilde{\mathbf{F}}_p \oplus \mathbf{F}_p = 1 \oplus \epsilon \oplus \chi.$$

C.Q.D.

Proposição 4. Seja Π, o pro–p–grupo livre em 4 geradores u, $\tau(u)$, $\tau^2(u)$, v. Defino uma A–ação em Π assim:

(a) $\tau(v) = v$ e τ permuta ciclicamente u, $\tau(u)$, $\tau^2(u)$, de maneira óbvia.

(b) $\sigma(u) = u$, $\sigma(v) = v^{-1}$.

Se $A \propto \Pi$ for o produto semidireto de Π por A com a ação acima, então existem isomorfismos fazendo o diagrama abaixo comutar:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Pi & \longrightarrow & A \propto \Pi & \longrightarrow & A & \longrightarrow & 1 \\ & & \cong \downarrow i & & i \downarrow \cong & & \downarrow id & & \\ 1 & \longrightarrow & P & \longrightarrow & G & \longrightarrow & A & \longrightarrow & 1 \end{array}$$

onde G é o p–completamento de $G_{Q,S}$ relativo a $\overline{\rho}$.

Prova: ([Bo-Ma]) É fácil ver que as prescrições (a) e (b) acima definem uma ação de A em Π, que induz no Frattini $\overline{\Pi}$ uma estrutura de A–módulo que é a mesma de $\overline{P}$. Já vimos no §3 do Capítulo 1 (antes do teorema 4) que para uma dada ação de A em $\overline{\Pi}$ só existe um produto semidireto (a menos de isomorfismo) entre A e Π. Isso prova a proposição.

Para a próxima proposição, vamos obter o análogo da proposição anterior, só que no caso local. Por isso, distinguimos duas situações: quando o grupo de decomposição em p, A_p, é cíclico de ordem 3, e cíclico de ordem 2.

Usaremos o mesmo símbolo, Π_p, para ambas as situações, para enfatizar o papel estrutural que ele vai desempenhar, dependendo de p.

Proposição 5. (a) Seja Π_p o pro–p–grupo livre em 4 geradores ξ, η, φ, ψ, com uma ação de $A_p = \{1, \tau, \tau^2\}$ dada por: τ fixa ξ, ψ e $\tau\eta = \varphi$, $\tau\varphi = \eta^{-1}\varphi^{-1}$.
(b) Seja Π_p o pro–p–grupo livre em 3 geradores ξ, η, φ com uma ação de $A_p = \{1, \sigma\}$, dada por: σ fixa ξ e φ e $\sigma\eta = \eta^{-1}$.

Então existe um diagrama comutativo (para cada caso)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Pi_p & \longrightarrow & A_p \propto \Pi_p & \longrightarrow & A_p & \longrightarrow & 1 \\ & & \cong\downarrow i & & \cong\downarrow i & & \| \mathrm{id} & & \\ 1 & \longrightarrow & P_p & \longrightarrow & G_p & \longrightarrow & A_p & \longrightarrow & 1 \end{array}$$

onde G_p é o p–completamento de G_{Q_p} relativo à $\overline{\rho}_p$ e ξ, η, φ (ξ, η no caso (b)) vão na inércia, via i.

Prova: A ação de A_p em Π_p induz um estrutura de $\mathbf{F}_p[A_p]$–módulo no Frattini $\overline{\Pi}_p$ que é (por construção) equivalente à estrutura de A_p–módulo de $\overline{P}_p$. Novamente, como só há um produto semidireto originando a ação no Frattini, temos os isomorfismos indicados. A segunda parte do enunciado é uma conseqüência do teorema 4 do §3 do Capítulo I.

C.Q.D.

Através dessas duas proposições acima, identificamos G com $A \propto \Pi$ e G_p com $A_p \propto \Pi_p$. O morfismo canônico $G_p \to G$ (§1 deste Capítulo) se restringe a um morfismo $\Pi_p \to \Pi$.

Proposição 6. Se o primo p for inerte na cúbica admissível K_1/Q (portanto, vale o

caso (a) da proposição 5) e denotarmos por r, s, t as imagens de ξ, η, $\varphi \in \Pi_p$ sob $\Pi_p \to \Pi$, teremos:

$$\overline{r} = \overline{v} + \overline{u} + \tau(\overline{u}) + \tau^2(\overline{u})$$

$$\overline{s} = \alpha.(\overline{u} - \tau\overline{u}) + \beta(\tau^2(\overline{u}) - \tau(\overline{u})$$

$$\overline{t} = \alpha.(\tau(\overline{u}) - \tau^2(\overline{u})) + \beta.(\overline{u} - \tau^2(\overline{u}))$$

Para certos α, β, em $\mathbf{F}_p$ onde a barra indica a redução no Frattini. Além disso, se $\overline{R}$ denotar A–módulo gerado por $\overline{r}$ e $\overline{S}$ denotar o A–módulo gerado por $\overline{s}$ então

$$\overline{R} \cong 1 \oplus \epsilon, \quad \overline{S} \simeq \chi.$$

Prova: Das proposições 3 e 4 sabemos que

$$\overline{\Pi} = < \overline{v} > \oplus < \overline{u} > \oplus < \tau\overline{u} > \oplus < \overline{\tau^2 u} >$$

como $\mathbf{F}_p$–espaço vetorial, onde

$$< \overline{v} > \cong \epsilon \quad \text{e} \quad < \overline{u} > \oplus < \overline{\tau(u)} > \oplus < \tau^2(\overline{u}) > \cong 1 \oplus \chi$$

como A–módulos. Como $\Pi_p \to \Pi$ é A_p–equivariante e τ fixa ξ, é claro que τ fixa $\overline{r}$ e portanto $\overline{r} = x.\overline{v} + y(\overline{u} + \overline{\tau(u)} + \overline{\tau^2(u)})$, onde x, $y \in \mathbf{F}_p$. Assim, $\overline{R} \subseteq 1 \oplus \epsilon$.

Como $\tau\overline{s} = \overline{t}$ e $\tau\overline{t} = -\overline{s} - \overline{t}$ uma conta simples mostra que

$$\overline{s} = \alpha.(\overline{u} - \tau(\overline{u})) + \beta.(\tau^2\overline{u} - \tau(\overline{u}))$$

$$\overline{t} = \alpha.(\tau\overline{u} - \tau^2\overline{u}) + \beta.(\tau\overline{u} - \tau^2\overline{u})$$

Pondo $k_1 = (\overline{u} - \tau(\overline{u}))$, $k_2 = (\tau^2(\overline{u}) - \tau(\overline{u}))$, $k_3 = (\tau(\overline{u}) - \tau^2(\overline{u}))$ e $k_4 = (\tau(\overline{u}) - \tau^2(\overline{u}))$, podemos facilmente determinar a ação de A:

$$\tau k_1 = -k_2 \qquad \sigma k_1 = k_1 - k_2$$

$$\tau k_2 = k_1 - k_2 \qquad \sigma k_2 = -k_2$$

É claro que os valores k_1 e k_2 são linearmente independentes e geram um subespaço A–invariante W bidimensional, com $W \cap \{1 \oplus \epsilon\} = (0)$, donde $W \cong \chi$. Como $\overline{S} \cong W$, $\overline{R} \subseteq 1 \oplus \epsilon$ e $\overline{R} + \overline{S} = \overline{\Pi}$, isso só é possível se $\overline{R} = 1 \oplus \epsilon$, $\overline{S} = \chi$.

C.Q.D.

Observação: (1) Como estamos trabalhando com as nossas representações iniciais, temos um morfismo A–equivariante

$$\oplus_{v|p} E_v / E_v^p \to \overline{P}$$

que é sobrejetor, donde o A–módulo gerado pela imagem da inércia em $\overline{P}$ é todo o $\overline{P}$. Por isso $\overline{R} + \overline{S} = \overline{\Pi}$.

(2) Mostramos que $\overline{R} = 1 \oplus \epsilon$, e em particular é bidimensional, de modo que na expressão de $\overline{r}$, $\overline{r} = x.\overline{v} + y.(\overline{u} + \tau^2(\overline{u}) + \tau(\overline{u}))$, x e y são ambos não nulos. Assim, por uma modificação apropriada de v e u, posso supor que $x = 1$, $y = 1$.

Retornando à seqüência exata de $\mathbf{F}_p[A]$–módulos

$$0 \to \overline{E} \to \oplus_{v|p} \overline{E}_v \to \overline{P} \to 0$$

que obtivemos pelo fato de (L, S) ser *neat* para p, e eliminando o Frattini dos primos sobre ℓ – que já observamos ser trivial –, consideremos os morfismos canônicos:

$$\overline{E} \xrightarrow{\Pi_v} \overline{E}_v.$$

Como esses morfismos canônicos são permutados transitivamente sob a ação de A, se denotarmos por d_v a dimensão da imagem de Π_v, vemos que $d_v = d$, independe de v (sobre p), e portanto só podemos ter dois casos:

(I) Caso genérico para p: $d = 2$

(II) Caso degenerado para p: $d = 1$.

A justificativa para essa terminologia provém do fato de que no caso tratado por Mazur [Bo-Ma], isto é, em que $\ell = p$, e portanto $S = \{\ell, \infty\}$, ele deu uma condição

necessária e suficiente para a ocorrência do caso degenerado, a saber:

$$\frac{1-(a/3)^{\ell-1}}{\ell} \equiv 4/3^5 \bmod \ell$$

onde a é o coeficiente do termo em X do polinômio X^3+aX+1. Não se conhece nenhum par, (a,ℓ), para o qual se verifique a congruência acima.

Proposição 7. Se a cúbica admissível K_1/Q tiver fecho Galoisiano L/Q genérico para p e $-\ell$ não for resíduo quadrático mod p (isto é, o caso (II)), podemos tomar um sistema local e global de geradores tal que sob o morfismo $\Pi_p \to \Pi$ a imagem de ξ é u e no Frattini, $\overline{\eta} = \overline{v} + 2.(\tau(\overline{u}) - \tau^2(\overline{u}))$.

Prova: (Ver Bo-Ma].) A única coisa a observar é que se $-\ell$ não for resíduo quadrático mod p, $A_p = \{1, \sigma^2\}$ e a prova do Mazur é a mesma, desde que L/Q seja genérico para p.

Até aqui, usando os resultados que obtivemos em II-2, caracterizamos Π e Π_p para todos os primos p (esses grupos encarnam os grupos de Galois relevantes, no caso global e local), bem como a sua ligação, através do mapa canônico $\Pi_p \to \Pi$.

Vamos agora calcular o anel universal das deformações e a deformação universal explicitamente. Como sempre (neste capítulo), seja K_1/Q uma cúbica admissível cujo fecho Galoisiano L/Q é o corpo de decomposição da representação residual

$$\overline{\rho} : G \to GL_2(\mathbf{F}_p)$$

construída como no §2.

Proposição 8. O anel universal $\mathbf{R}$ de $\overline{\rho}$ pode ser identificado com $\mathbf{Z}_p[[T_1, T_2, T_3]]$ e podemos dar a seguinte descrição da deformação universal ρ:

$$\rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \rho(\tau) = \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix} \qquad \rho(u) = \begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix}$$

$$\rho(v) = \begin{pmatrix} (1-3T_3^2)^{1/2} & T_3 \\ -3T_3 & (1-3T_3^2)^{1/2} \end{pmatrix}$$

Prova: Ver [Bo-Ma], pg.23.

Novamente observamos que Mazur faz as coisas para $\ell = p$. Porém a prova é a mesma, decorrendo dos métodos desenvolvidos em [Bo], e utilizando apenas a descrição de Π como A–módulo.

II-4 - Em Busca de Deformações Ordinárias

No §2 do Capítulo I definimos a noção geral de deformação ordinária relativa a um subgrupo fechado $I \subset G$. No Capítulo III passamos a chamar de deformações ordinárias aquelas em que o subgrupo fechado I era o subgrupo de inércia (selvagem) em p. Ali, as representações residuais são ordinárias, o que já não ocorre na nossa situação, pois p não ramifica em L, e portanto o subgrupo de inércia em p, na extensão L, é trivial.

Se quisermos encontrar deformações de $\overline{\rho}$ que sejam ordinárias, inicialmente precisamos achar sub módulos livres de posto 1 que fiquem fixos pela inércia. Antes de passarmos a isso, é conveniente interpretar o espaço universal das deformações de $\overline{\rho}$ (para $\mathbf{Z}_p$) como uma variedade analítica p–ádica de dimensão 3 por meio da identificação:

$$X = \mathrm{Hom}(\mathbf{Z}_p[[T_1, T_2, T_3]], \mathbf{Z}_p) \xrightarrow{\cong} p\mathbf{Z}_p \times p\mathbf{Z}_p \times p\mathbf{Z}_p$$

$$x \mapsto (x(T_1), x(T_2), x(T_3))$$

A cada $x \in X$ temos uma representação $\rho_x : G \to GL_2(\mathbf{Z}_p)$ induzida por x e pela deformação universal de $\overline{\rho}$.

Vamos começar com o caso em que p é inerte na cúbica K_1/Q. Neste caso, $A_p = \{1, \tau, \tau^2\}$ e a proposição 5 garante a existência de 4 geradores ξ, η, φ, ψ de Π_p com a ação de A_p: τ fixa ξ e ψ, $\tau(\eta) = \varphi$, $\tau(\varphi) = \eta^{-1}\varphi^{-1}$, e ξ, η, φ estão na inércia. Se r, s, t são as imagens de ξ, η, φ em Π, via $\Pi_p \to \Pi$, a proposição 6 nos dá uma descrição das projeções $\overline{r}$, $\overline{s}$ e $\overline{t}$ no Frattini de Π.

Se ρ denota a deformação universal, vamos denotar por

$$\rho(r) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

a imagem de r. Como $\tau(r) = r$, $\rho(\tau(r)) = \rho(r)$ e como ρ é A–equivariante, $\rho(\tau(r)) = \rho(\tau)\rho(r)\rho(\tau)^{-1}$. Utilizando a proposição 8 e fazendo uma conta simples, vemos que

$$\rho(r) = \begin{pmatrix} 1+f & g \\ -3g & 1+f \end{pmatrix}$$

onde $f, g \in \mathcal{M}$, o ideal maximal de $\mathbf{Z}_p[[T_1, T_2, T_3]]$.

Para termos um conhecimento melhor de f e g, vamos calcular suas imagens módulo $\mathcal{M}^2$. É fácil ver que o kernel da projeção natural

$$GL_2(\mathbf{Z}_p[[T_1, T_2, T_3]]/\mathcal{M}^2) \to GL_2(\mathbf{F}_p)$$

é um grupo abeliano p–elementar, e portanto o homomorfismo

$$\rho : P \to GL_2(\mathbf{Z}_p[[T_1, T_2, T_3]])$$

induz um morfismo no Frattini

$$\widetilde{\rho} : \overline{P} \to GL_2(\mathbf{Z}_p[[T_1, T_2, T_3]]/\mathcal{M}^2).$$

Pela proposição 6,

$$\widetilde{\rho}(\overline{r}) = \widetilde{\rho}(v) + [\widetilde{\rho}(\overline{u}) + \widetilde{\rho}(\tau(\overline{u})) + \widetilde{\rho}(\tau^2(\overline{u}))],$$

ou seja,

$$\widetilde{\rho}(\overline{r}) = \begin{pmatrix} 1 & T_3 \\ -3T_3 & 1 \end{pmatrix} + \left[\begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} 4+T_1+3T_2 & T_1-T_2 \\ 3T_1-3T_2 & 4+3T_1+T_2 \end{pmatrix} \right.$$

$$\left. + \frac{1}{4} \begin{pmatrix} 4+3T_2+T_1 & T_2-T_1 \\ -3T_1+3T_2 & 4+3T_1+T_2 \end{pmatrix} \right]$$

e portanto

$$\widetilde{\rho}(\overline{r}) = \begin{pmatrix} 1+\frac{3}{2}(T_1+T_2) & T_3 \\ -3T_3 & 1+\frac{3}{2}(T_1+T_2) \end{pmatrix} \bmod (\mathcal{M}^2)$$

Observação: As contas de fato fazem sentido, pois no kernel acima citado a operação de grupo é facilmente calculada em termos dessa "soma" especial de matrizes que fizemos acima.

Assim,

$$f \equiv \frac{3}{2}(T_1+T_2) \bmod \mathcal{M}^2$$

$$g \equiv T_3 \bmod \mathcal{M}^2$$

e como f, g estão em $\mathcal{M}$, é claro que suas projeções em $\mathcal{M}/\mathcal{M}^2$ são linearmente independentes.

Vamos agora considerar deformações de $\overline{\rho}$ para $\mathbf{Z}_p$, isto é, pontos de $X = \mathrm{Hom}(\mathbf{Z}_p[[T_1,T_2,T_3]],\mathbf{Z}_p)$. É claro que se $x \in X$, pensamos na representação $\rho_x : G \to GL_2(\mathbf{Z}_p)$ induzida por x e pela deformação universal de $\overline{\rho}$. Assim, em termos matriciais, ρ_x é obtida por especificação das variáveis T_1, T_2, T_3, nas entradas das matrizes da deformação universal de $\overline{\rho}$. Recordo também que $X \cong p\mathbf{Z}_p \times p\mathbf{Z}_p \times p\mathbf{Z}_p$ via $x \mapsto (x(T_1), x(T_2), x(T_3))$.

O polinômio característico de $\rho_x(r)$ é

$$\lambda^2 - 2(1+f)\lambda + (1+f)^2 + 3g^2$$

(onde já estou usando f e g para a especificação correspondente a x) e suas raízes são $\lambda_{1,2} = (1+f) \pm g.\sqrt{-3})$.

Suponhamos que 1 seja autovalor de $\rho_x(r)$. Neste caso

$$1 = (1+f) \pm g\sqrt{-3}$$

e portanto ou $f = g\sqrt{-3}$ ou $f = -g\sqrt{3}$.

Temos portanto duas possibilidades: para o vetor fixo (no caso de $g \neq 0$): se $f = \sqrt{-3}g$, $\rho_x(r)$ pode fixar $V_x = (1, -\sqrt{-3})$ e se $f = -\sqrt{-3}g$, $\rho_x(r)$ pode fixar $V_x = (1, \sqrt{-3})$. Se $g = 0$ (e conseqüentemente $f = 0$), $\rho_x(r)$ é identidade.

Tomemos agora as matrizes dos outros elementos da inércia; em $GL_2(\mathbf{Z}_p[[T_1, T_2, T_3]])$

$$\rho(s) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = A \qquad \rho(t) = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = B \ .$$

Como $\tau s = t$ e $\rho(\tau(s)) = \rho(\tau)\rho(s)\rho(\tau)^{-1} = \rho(t)$, utilizando a proposição 8 e fazendo a conta acima, concluímos que

$$(*) \qquad \begin{array}{ll} a_2 = (a_1 - 3b_1 - c_1 + 3d_1)/4 & b_2 = (a_1 + b_1 - c_1 - d_1)/4 \\ c_2 = (3a_1 - 9b_1 + c_1 - 3d_1)/4 & d_2 = (3a_1 + 3b_1 + c_1 + d_1)/4 \end{array}$$

Observe que $a_1 \equiv d_1 \equiv 1 \bmod \mathcal{M}$ e $b_1 \equiv c_1 \equiv 0 \bmod \mathcal{M}$.

Como $\tau t = s^{-1}t^{-1}$, $\tau B \tau^{-1} = A^{-1}B^{-1}$ e como $\tau A \tau^{-1} = B$, $\tau^{-1} A \tau = A^{-1}B^{-1}$. Essa equação matricial fica:

$$\begin{pmatrix} -1/2 & -1/2 \\ 3/2 & -1/2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix} = \frac{1}{\Delta^2} \cdot \begin{pmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{pmatrix} \begin{pmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{pmatrix}$$

onde $\Delta = \det A = (\det A)^{-1}.\det(B)^{-1} = \det B$ (note que $\Delta^3 = 1$).

Desenvolvendo e utilizando $(*)$ acima, obtemos:

$$\begin{cases} (a_1 + 3b_1 + c_1 + 3d_1)\Delta^2 = \Big[(b_1 + d_1)(3a_1 + c_1) + (d_1 + 3b_1)(d_1 - 3b_1)\Big] \\ (-a_1 + b_1 - c_1 + d_1)\Delta^2 = \Big[(b_1 + d_1)(c_1 - a_1) - 4b_1 d_1 + d_1^2 + 3b_1^2\Big] \\ (-3a_1 - 9b_1 + c_1 + 3d_1)\Delta^2 = \Big[(d_1 + 3b_1)(3a_1 - c_1) - a_1(4c_1 + 3a_1) - c_1^2\Big] \\ (3a_1 - 3b_1 - c_1 + d_1)\Delta^2 = \Big[(c_1 - 3a_1)(b_1 - d_1) + (a_1 - c_1)(a_1 + c_1)\Big] \end{cases}$$

Lema 1. No sistema acima, se $a_1 = 1$ então $d_1 = 1$ e $b_1 = c_1 = 0$.

Prova: Já sabemos que $a_1 \equiv d_1 \equiv 1 \bmod \mathcal{M}$, $b_1 \equiv c_1 \equiv 0 \bmod \mathcal{M}$. Suponhamos inicialmente que $b_1 = 0$. A primeira equação do sistema nos dá:

$$(1 + c_1 + 3d_1)d_1^2 = [d_1(3 + c_1) + d_1^2],$$

ou seja, $c_1 d_1^2 + 3d_1^3 = 3d_1 + d_1 c_1$. Como $d_1 \equiv 1 \bmod \mathcal{M}$, $d_1 \neq 0$, donde $c_1 d_1 + 3d_1^2 = 3 + c_1$, ou seja, $3(d_1^2 - 1) = c_1(1 - d_1)$. Porém $c_1 \in \mathcal{M}$ e $(1 - d_1) \in \mathcal{M}$, donde $3(d_1^2 - 1) \in \mathcal{M}^2$, ou ainda $(d_1^2 - 1) \in \mathcal{M}^2$. Pondo $\widetilde{d_1} = d_1 - 1$, $\widetilde{d_1} \in \mathcal{M}$ e $(d_1^2 - 1) = (1 + \widetilde{d_1})^2 - 1 = 1 + 2\widetilde{d_1} + \widetilde{d_1^2} - 1 = 2\widetilde{d_1} + \widetilde{d_1^2}$. Portanto $2\widetilde{d_1} \in \mathcal{M}^2$, ou seja, $\widetilde{d_1} \in \mathcal{M}^2$. Na proposição seguinte, daremos uma caracterização explícita para $\widetilde{d_1} (\bmod \mathcal{M}^2)$ e veremos que isso só é possível se $\widetilde{d_1} = 0$, e conseqüentemente, se $b_1 = 0$, então $d_1 = 1$.

Somemos agora a 1a. e a 4a. equações do nosso sistema:

$$4(1 + d_1)(d_1^2 - 2d_1 b_1 c_1 + b_1^2 c_1^2) = [6d_1 + 2b_1 c_1 + d_1^2 - 9b_1^2 + 1 - c_1^2].$$

Reduzindo módulo $\mathcal{M}^2$, obtemos

$$4(1 + d_1)d_1^2 \equiv (6d_1 + d_1^2 + 1) \bmod \mathcal{M}^2,$$

ou, em função de $\widetilde{d_1}$ (que pertence a $\mathcal{M}$):

$$\begin{aligned} &4(2 + \widetilde{d_1})(1 + \widetilde{d_1})^2 \equiv (6(1 + \widetilde{d_1}) + (1 + \widetilde{d_1})^2 + 1) \bmod \mathcal{M}^2 \\ &4(2 + \widetilde{d_1})(1 + 2\widetilde{d_1}) \equiv (8 + 8\widetilde{d_1}) \bmod \mathcal{M}^2 \\ &8 + 20\widetilde{d_1} \equiv 8 + 8\widetilde{d_1} \bmod \mathcal{M}^2 \end{aligned} \quad ,$$

ou seja, $12\widetilde{d_1} \in \mathcal{M}^2$, isto é, $\widetilde{d_1} \in \mathcal{M}^2$. Assim, $a_1 = 1$ implica $\widetilde{d_1} \in \mathcal{M}^2$ e isso só é possível se $d_1 = 1$.

Reescrevamos o nosso sistema com $a_1 = 1$, $d_1 = 1$, e reduzamos $\bmod \mathcal{M}^2$:

$$\begin{cases} (4 + 3b_1 + c_1) \equiv (3b_1 + 4) \bmod \mathcal{M}^2 \\ (b_1 - c_1) \equiv (-5b_1 + c_1) \bmod \mathcal{M}^2 \\ (-9b_1 + c_1) \equiv (9b_1 - 5c_1) \bmod \mathcal{M}^2 \\ (4 - 3b_1 - c_1) \equiv (-c_1 - 3b_1 + 4) \bmod \mathcal{M}^2 \end{cases}$$

Da primeira equação vimos que $c_1 \equiv 0 \bmod \mathcal{M}^2$ e da segunda equação sai que $6b_1 \equiv 2c_1 \equiv 0 \bmod \mathcal{M}^2$.

Pela próxima proposição, isso só é possível se $c_1 = b_1 = 0$.

C.Q.D.

Proposição 1. Pondo $d_1 = 1 + \widetilde{d_1}$, $a_1 = 1 + \widetilde{a_1}$, então

$$\widetilde{a_1} = \frac{3}{4}.\alpha.(T_1 - T_2).\text{mod } \mathcal{M}^2$$

$$b_1 \equiv (\alpha + 2\beta)(T_2 - T_1)/4 \text{ mod } \mathcal{M}^2$$

$$c_1 \equiv 3(\alpha + 2\beta)(T_2 - T_1)/4 \text{ mod } \mathcal{M}^2$$

$$\widetilde{d_1} \equiv \frac{3}{4}.\alpha.(T_2 - T_1) \text{ mod } \mathcal{M}^2$$

onde α e β são os coeficientes que aparecem nas expressões de $\bar{s}$ e $\bar{t}$ da proposição 6 do §3.

Prova: Assim como fizemos para o cálculo de $\widetilde{\rho}(\bar{r})$, onde $\widetilde{\rho} : \overline{P} \to GL_2(\mathbf{Z}p[[T_1, T_2, T_3]]/\mathcal{M}^2)$, pela proposição 6 do §3, sabemos que

$$\bar{s} = \alpha(\bar{u} - \tau\bar{u}) + \beta(\tau^2(\bar{u}) - \tau(\bar{u})), \quad \alpha, \beta \in \mathbf{F}_p,$$

donde

$$\widetilde{\rho}(\bar{s}) = \alpha \left[\begin{pmatrix} 1+T_1 & 0 \\ 0 & 1+T_2 \end{pmatrix} - \frac{1}{4} \begin{pmatrix} 4+T_1+3T_2 & T_1-T_2 \\ 3(T_1-T_2) & 4+3T_1+T_2 \end{pmatrix} \right] +$$

$$+\beta \left[\begin{pmatrix} 4+T_1+3T_2 & T_2-T_1 \\ 3(T_2-T_1) & 4+3T_1+T_2 \end{pmatrix} \frac{1}{4} - \tau(\bar{u}) \right]$$

$$\widetilde{\rho}(\bar{s}) = \alpha. \left[\begin{pmatrix} 1+\frac{3}{4}(T_1-T_2) & (T_2-T_1)/4 \\ \frac{3}{4}(T_2-T_1) & 1+\frac{3}{4}(T_2-T_1) \end{pmatrix} \right] + \beta. \begin{pmatrix} 1 & (T_2-T_1)/2 \\ 3(T_2-T_1)/2 & 1 \end{pmatrix}$$

$$\widetilde{\rho}(\bar{s}) = \begin{pmatrix} 1+\alpha.\frac{3}{4}(T_1-T_2) & (\alpha+2\beta)(T_2-T_1)/4 \\ 3(\alpha+2\beta)(T_2-T_1)/4 & 1+\frac{3}{4}\alpha.(T_2-T_1) \end{pmatrix} \text{mod } \mathcal{M}^2$$

o que implica a proposição.

C.Q.D.

Feito esse trabalho preliminar, procuremos agora um vetor $\neq 0$ que seja fixado por A e B (nas correspondentes especificações para $\mathbf{Z}_p$). Seja v tal vetor. Assim, se

$Av = v$ e $Bv = v$, como $\tau A \tau^{-1} = B$ (estamos abreviando $\rho(\tau)$ para τ) segue que $\tau A \tau^{-1} v = v$, donde $A\tau^{-1}v = \tau^{-1}v$, e portanto v e $\tau^{-1}v$ são vetores fixos pela matriz A. Conseqüentemente, se $\tau^{-1}v \neq \lambda v$ para todo $\lambda \in \mathbf{Z}_p$, $\lambda \neq 0$, então a matriz A é necessariamente a identidade (e portanto B também reduz-se à identidade).

Se, por outro lado, v for um autovetor para $\rho(\tau)$, como $\tau^3 = 1$, os possíveis autovalores para $\rho(\tau)$ são as raízes cúbicas não triviais da unidade, ω, ω^2. Portanto, se $\omega \notin \mathbf{F}_p$ (e portanto $\omega \notin \mathbf{Z}_p$), A e B não fixam nada além da origem. Se $\omega \in \mathbf{F}_p$, os únicos possíveis candidatos a serem fixos são v_1 e v_2, onde $\rho_x(\tau)v_1 = \omega v_1$ e $\rho_x(\tau)v_2 = \omega^2 v_2$. Da proposição 8,

$$\rho_x(\tau) = \begin{pmatrix} -1/2 & 1/2 \\ -3/2 & -1/2 \end{pmatrix}$$

e portanto $v_1 = (1 + 2\omega, -3)$, $v_2 = (1 + 2\omega, +3)$.

Se

$$\begin{pmatrix} 1 + \widetilde{a_1} & b_1 \\ c_1 & 1 + \widetilde{d_1} \end{pmatrix} \begin{pmatrix} 1 + 2\omega \\ -3 \end{pmatrix} = \begin{pmatrix} 1 + 2\omega \\ -3 \end{pmatrix},$$

então $\widetilde{a_1}(1 + 2\omega) = +3b_1$ e $c_1(1 + 2\omega) = +3\widetilde{d_1}$. Analogamente, usando agora v_2 em vez de v_1, obtemos

$$\widetilde{a_1}(1 + 2\omega) = -3b_1 \quad \text{e} \quad c_1(1 + 2\omega) = -3\widetilde{d_1}\ .$$

Assim, sendo 1 autovalor de A, substituindo λ por 1 no seu polinômio característico, obtemos

$$1 - (a_1 + d_1) + (a_1 d_1 - b_1 c_1) = 0$$

e portanto, se $\widetilde{a_1}(1 + 2\omega) = -3b_1$ (ou, multiplicando ambos os membros por $(1 + 2\omega)$ e lembrando que $1 + \omega + \omega^2 = 0$, $\widetilde{a_1} = (1 + 2\omega)b_1$), substituindo vem:

$$1 - (1 + (1 + 2\omega)b_1 + d_1) + (1 + (1 + 2\omega)b_1)d_1 - b_1 c_1 = 0,$$

ou seja,

$$(1 + 2\omega)d_1 b_1 - b_1 c_1 = (1 + 2\omega)b_1;$$

se $b_1 \neq 0$, ficamos com

$$(1+2\omega)d_1 - c_1 = (1+2\omega),$$

ou, $(1+2\omega)(1+\widetilde{d_1}) - c_1 = (1+2\omega)$, que se escreve como

$$(1+2\omega)\widetilde{d_1} = c_1$$

multiplicando ambos os lados por $(1+2\omega)$, vem

$$c_1(1+2\omega) = -3\widetilde{d_1}.$$

Observação: Se utilizarmos a relação proveniente de v_1, obteremos o resultado análogo correspondente.

Vamos fazer um resumo geral da situação neste caso de p inerte na cúbica:

1) $\rho_x(r)$ tem as seguintes possibilidades:
   a) $\sqrt{-3} = (1+2\omega) \notin \mathbf{F}_p$. Neste caso, $\rho_x(r)$ não pode ter vetor fixo diferente do trivial.
   b) $\sqrt{-3} \in \mathbf{F}_p$, mas $g = 0$. Neste caso, para ter um vetor fixo não trivial, $f = 0$ e $\rho_x(r)$ é a identidade.
   c) $\sqrt{-3} \in \mathbf{F}_p$ e $g \neq 0$. Temos dois casos:
      c.1) $f = (1+2\omega)g$. Aqui o único vetor $\neq 0$ que pode ser fixo por r é $V = (-1, (1+2\omega))$,
      c.2) $-f = (1+2\omega)g$. Aqui o único vetor $\neq 0$ que pode ser fixo por r é $V = (1, (1+2\omega))$.

2) $\rho_x(s) = A$ e $\rho_x(t) = B$ têm as seguintes possibilidades:
   a) $\sqrt{-3} = (1+2\omega) \notin \mathbf{F}_p$. Neste caso, A e B não fixam nada além da origem, a menos que $A = B =$ identidade.
   b) $\sqrt{-3} = (1+2\omega) \in \mathbf{F}_p$. Neste caso, os candidatos a vetor fixo não trivial são $v_1 = (1+2\omega, -3)$ e $v_2 = (1+2\omega, +3)$.

Podemos agora enunciar o

Teorema 1. Suponhamos que p seja inerte na cúbica admissível e ρ_x uma deformação de $\overline{\rho}$ para $\mathbf{Z}_p$ induzida por $x \in X$.

a) Se $\mathbf{F}_p$ não contiver uma raiz cúbica não trivial da unidade, então não existem deformações ρ_x tais que a inércia em p fixe um vetor não trivial de $\mathbf{Z}_p \times \mathbf{Z}_p$.

b) Se $\mathbf{F}_p$ contiver um raiz cúbica ω não trivial da unidade temos as seguintes possibilidades:

b.1) $g = 0$ e $f = 0$ e $\widetilde{a_1}(1+2\omega) = 3b_1$ e $c_1(1+2\omega) = 3\widetilde{d_1}$ dão deformações ordinárias fixando $v_1 = (1+2\omega, -3)$.

b.2) $g = 0$ e $f = 0$ e $\widetilde{a_1}(1+2\omega) = -3b_1$ e $c_1(1+2\omega) = -3\widetilde{d_1}$ dão deformações ordinárias fixando $v_2 = (1+2\omega, 3)$.

b.3) $g \neq 0$ e $f = (1+2\omega)g$ e $a_1 = 1$, então temos deformações ordinárias fixando $v = (-1, (1+2\omega))$.

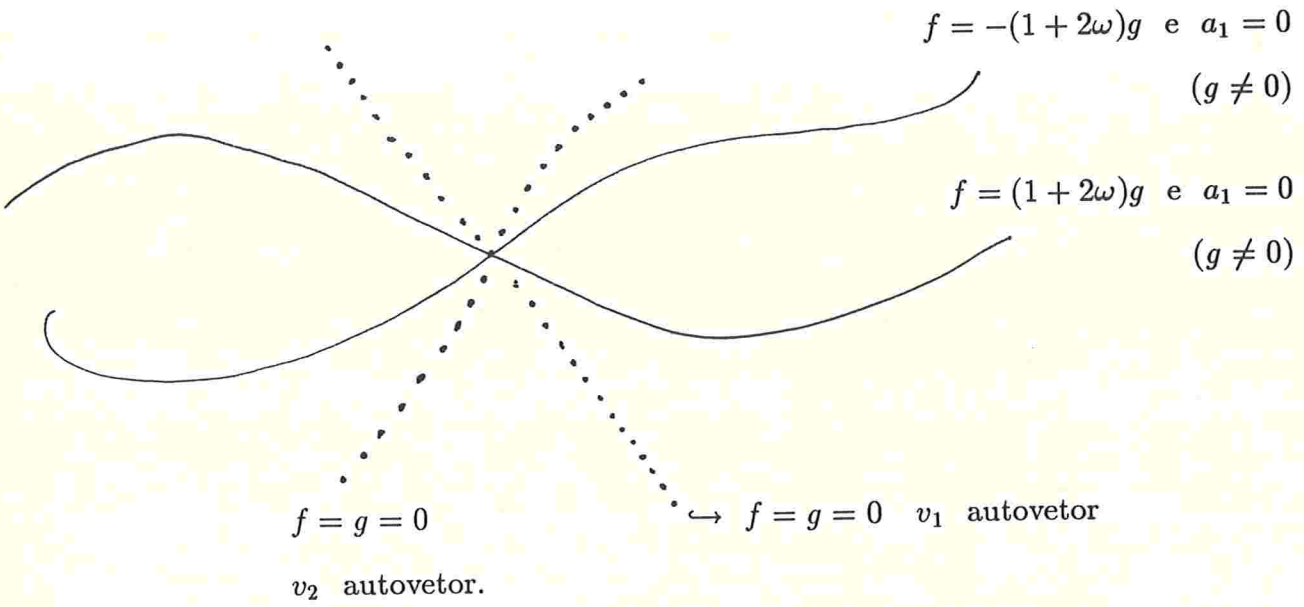
b.4) $g \neq 0$ e $-f = (1+2\omega)g$ e $a_1 = 1$, então temos deformações ordinárias fixando $v = (1, (1+2\omega))$.

Observação: 1) Nos itens b.1) e b.2), se $b_1 \neq 0$, temos apenas duas condições: $g = 0$ e $\widetilde{a_1}(1+2\omega) = 3b_1$ para b.1) e $g = 0$ e $\widetilde{a_1}(1+2\omega) = -3b_1$ para b.2), como já observamos antes.

2) Para obtermos deformações ρ_x *não ramificadas* em p, precisamos que $f = g = 0$ e $a_1 = 1$, (veja-se o lema 1 atrás).

3) O lugar geométrico dado em b.1) e o lugar dado em b.2) se encontram no lugar das não ramificadas, que por sua vez está no fecho de b.3) e de b.4).

A figura que isso daria é semelhante a:



Assim, na situação do teorema 1, vemos que o lugar das deformações ordinárias não é um subesquema fechado.

Procuremos agora analisar o caso em que $-\ell$ não é resíduo quadrático módulo p. Agora $A_p = \{1, \sigma\}$, e estamos também supondo que L/Q é genérico para p, ou seja, na situação da proposição 7 do §3, e portanto a imagem de ξ é u e no Frattini $\overline{\eta} = \overline{v} + 2(\tau(\overline{u}) - \tau^2(\overline{u}))$. Neste caso, já conhecemos $\rho(u)$, e é fácil ver que

$$\rho(\eta) = \begin{pmatrix} (1+fg)^{1/2} & f \\ g & (1+fg)^{1/2} \end{pmatrix}.$$

De fato, como $\sigma\eta = \eta^{-1}$, $\rho(\sigma\eta) = \rho(\sigma)\rho(\eta)\rho(\sigma)^{-1}$. Pondo

$$\rho(\eta) = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \Gamma_2(\mathbf{R}),$$

vemos que $\det\rho(\eta) = 1$, pois $\sigma\eta = \eta^{-1}$, e sua redução para $GL_2(\mathbf{F}_p)$ é a identidade. Assim,

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} w & -y \\ -z & x \end{pmatrix}$$

Isso nos dá imediatamente $x = w$, e o determinante fica $x^2 - zy = 1$, donde $x = (1+zy)^{1/2}$, o que queríamos. Os autovalores de $\rho(\eta)$ são $\lambda_{1,2} = (1+fg)^{1/2} \pm (fg)^{1/2}$

e portanto 1 será autovalor se

$$1 = (1+fg)^{1/2} + (fg)^{1/2} \quad \text{ou} \quad 1 = (1+fg)^{1/2} - (fg)^{1/2}.$$

Em ambos os casos isso acarreta ou $f = 0$ ou $g = 0$.

Se $f = 0$, a única possibilidade é fixar $(0,1)$ e portanto, se $\rho(u)$ fixar $(0,1)$, $T_2 = 0$. Se $g = 0$, então $T_1 = 0$, e temos o lugar dos morfismo ordinários:

$$f = 0 \quad \text{e} \quad T_2 = 0 \quad \text{ou (exclusivo)} \quad g = 0 \quad \text{e} \quad T_1 = 0.$$

Além disso, as imagens de f e T_2 (resp. g e T_1) em $\mathcal{M}/\mathcal{M}^2$ são linearmente independentes. Isso sai diretamente da proposição 7, que diz que $\overline{\eta} = \overline{v} + 2.(\tau(\overline{u}) - \tau^2(\overline{u}))$, ou seja,

$$f \equiv T_1 - T_2 + T_3 \bmod \mathcal{M}^2$$

$$g \equiv 3T_1 - 3T_2 - 3T_2 \bmod \mathcal{M}^2$$

.

Resumindo:

Teorema 2. Se L/Q for genérica para p e $-\ell$ não for resíduo quadrático mod p, então uma deformação ρ de $\overline{\rho}$ para $\mathbf{Z}_p$ é ordinária se $f = 0$ e $T_1 = 0$ ou (exclusivo) $g = 0$ e $T_2 = 0$.

Teorema 3. Se L/Q for degenerada para p e $-\ell$ não for resíduo quadrático mod p, então se ρ for uma deformação ordinária de $\overline{\rho}$ para $\mathbf{Z}p$, temos (exclusivamente), ou $x = 0$ e $f = 0$ ou $x = 0$ e $g = 0$ ou $T_1 = 0$ e $T_3 = 0$ ou $T_2 = 0$ e $T_3 = 0$.

Prova: Da proposição 5, (b) (§3), sabemos que Π_p é um pro–p–grupo livre em 3 geradores ξ, η, φ com a ação de $A_p = \{1, \sigma\}$. Assim: $\sigma\xi = \xi$, $\sigma\eta = \eta^{-1}$. Denotemos por r e s as imagens de ξ, η em Π e por $\overline{R}$ o A–módulo gerado por $\overline{r}$, e por $\overline{S}$ o A–módulo gerado por $\overline{s}$, no Frattini $\overline{\Pi}$. Como $\sigma\overline{r} = \overline{r}$, $\overline{r} \in 1 \oplus \chi$ donde $\overline{R} \subseteq 1 \oplus \chi$. Do mesmo modo, $\sigma\overline{s} = -\overline{s}$ implica $\overline{S} \subseteq \epsilon \oplus \chi$. Como já vimos na observação que se segue à

prova da proposição 6, $\overline{R}+\overline{S}=\overline{\Pi}$, donde, se L/Q for degenerada para p, temos duas possibilidades:

Ou $\overline{R}=1$ e $\overline{S}=\epsilon\oplus\chi$ ou $\overline{S}=\epsilon$ e $\overline{R}=1\oplus\chi$.

No primeiro caso, o teorema 4 do §3 do Capítulo I me garante que A age trivialmente em $r\in\Pi$: $\sigma r=r$, $\tau r=r$ e no caso de s, temos $\overline{s}=\overline{v}+2(\tau\overline{u}-\tau^2\overline{u})$, como na proposição 7 do §3. Por ser invariante sob σ, $\rho(r)$ tem que ser uma matriz diagonal, e por ser fixa por τ,

$$\rho(r)=\begin{pmatrix}1+x & 0\\ 0 & 1+x\end{pmatrix}.$$

Quanto a $\rho(s)$, já fizemos o cálculo anteriormente:

$$\rho(s)=\begin{pmatrix}(1+fg)^{1/2} & f\\ g & (1+fg)^{1/2}\end{pmatrix}.$$

E portanto temos duas únicas formas da inércia fixar um vetor (sem ser trivial):

ou $x=0$ e $f=0$, ou $x=0$ e $g=0$.

No segundo caso, $\overline{s}=\overline{v}$ e posso escolher $v=s$, de modo que

$$\rho(s)=\begin{pmatrix}(1-2T_3^2)^{1/2} & T_3\\ -3T_3 & (1-3T_3^2)^{1/2}\end{pmatrix}$$

e $\overline{R}=1\oplus\chi$, de modo que $\overline{r}$, $\tau\overline{r}$, $\tau^2\overline{r}$ são linearmente independentes e $\sigma\overline{r}=\overline{r}$. Pelo Adendo da proposição 7 em §2.2 de [Bo-Ma], posso escolher u como a imagem de ξ, isto é, $r=u$, ou seja,

$$\rho(r)=\begin{pmatrix}1+T_1 & 0\\ 0 & 1+T_2\end{pmatrix}$$

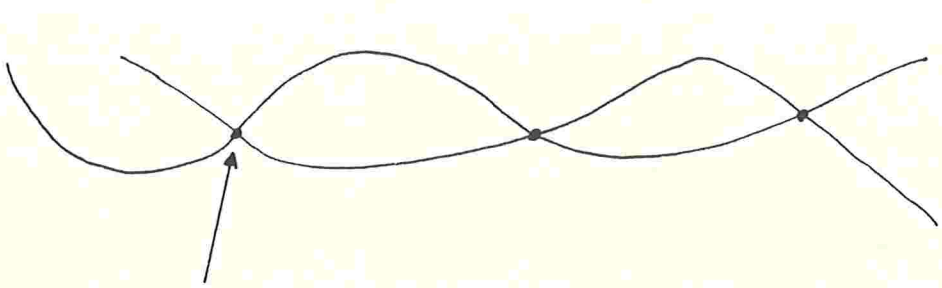
e portanto a inércia fixará um (e um só vetor) se

$T_1=0$ e $T_3=0$ ou (exclusivo) se $T_2=0$ e $T_3=0$.

C.Q.D.

Assim, as possíveis figuras nesses casos seriam:

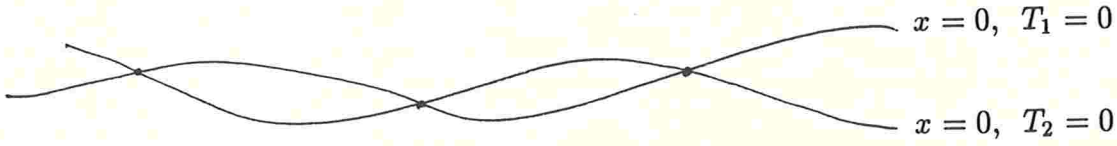
1) Caso genérico:



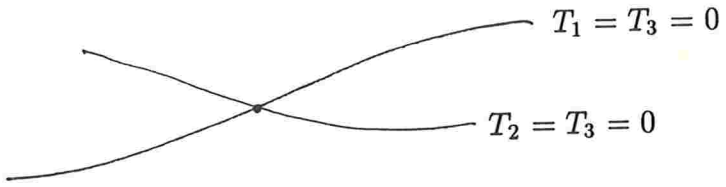
o lugar não ramificado

2) Caso degenerado:

2.1)



2.2)



CAPÍTULO III

DEFORMAÇÕES DE REPRESENTAÇÕES ORDINÁRIAS NÃO RAMIFICADAS FORA DE p

Neste capítulo nosso objetivo é provar o

Teorema Principal. Seja $\overline{\rho} : \mathrm{Gal}(\overline{Q}/Q) \to GL_2(k)$ uma representação contínua absolutamente irredutível, ordinária, não ramificada fora de $S = \{p, \infty\}$. Então o homomorfismo natural

$$\mathbf{R}(\overline{\rho}, S) \to \mathbf{R}^0(\overline{\rho}, S)$$

é sobrejetor e se $\overline{\rho}$ for moderadamente ramificada, o seu kernel pode ser gerado por dois elementos.

Será útil recordar aqui que $G_{Q,S}$ denota o grupo de Galois do maior subcorpo de $\overline{Q}$ que é não ramificado fora de S e k é um corpo finito de característica p. É conveniente que denotemos por G_F o grupo de Galois da maior extensão algébrica separável de um corpo F. Poremos também $G := \mathrm{Gal}(L/Q)$ onde L é o corpo de decomposição de $\overline{\rho}$, isto é, o corpo fixo de $\mathrm{Ker}\ \overline{\rho}$, e denotaremos por Π o p–completamento de $G_{Q,S}$ relativo a $\overline{\rho}$ (cf. definição em I-3).

Temos a seqüência exata curta:

$$1 \longrightarrow P \longrightarrow \Pi \xrightarrow{\overline{\rho}} G \longrightarrow 1$$

onde P é um pro–p–subgrupo normal de Π, que é grupo de Galois da maior pro–p–extensão de L, não ramificada fora de S. Já vimos em I-3 que todas as deformações de $\overline{\rho}$ se "fatoram" por Π. Fixemos uma imersão $\overline{Q} \hookrightarrow \overline{Q}_p$ entre o fecho algébrico dos racionais e o fecho algébrico dos racionais p–ádicos, e consideremos os grupos de inércia e decomposição correspondentes, $I \subset D \subset \Pi$, de modo que I é a imagem do subgrupo de

inércia de G_{Q_p} em Π e D é a imagem de todo G_{Q_p} (via o morfismo $v : G_{Q_p} \hookrightarrow G_Q$ induzido pela imersão fixada acima).

Sejam $I^0 \subset I$ e $D^0 \subset D$ as pro–p–subgrupos de Sylow de I e D. Como $\overline{\rho}$ é ordinária, pela propriedade (a) de I-1, posso supor sem perda de generalidade que

$$\overline{\rho}(I) \subseteq \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

e portanto $\overline{\rho}(D)$ está contido num subgrupo de Borel

$$\overline{\rho}(D) \subseteq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

de $GL_2(k)$. Esse subgrupo de Borel se escreve como o produto semidireto do grupo das matrizes diagonais pelo grupo das unipotentes,

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} \begin{pmatrix} 1 & y/x \\ 0 & 1 \end{pmatrix}$$

Assim, se restringirmos a seqüência exata acima, obteremos

$$1 \longrightarrow D_1 \longrightarrow D \longrightarrow \overline{\rho}(D) \longrightarrow 1$$

onde observamos que como $D_1 \subseteq P$, então $D_1 \subseteq D^0$ e assim

$$1 \longrightarrow D_1 \longrightarrow D^0 \longrightarrow \overline{\rho}(D^0) \longrightarrow 1$$

é também exata. Conseqüentemente, como $\overline{\rho}(D^0) = \overline{\rho}(D) \cap$ (unipotentes), temos que $\overline{\rho}(D^0) \lhd \overline{\rho}(D)$ e portanto $D^0 \lhd D$. Analogamente, temos que $I^0 \lhd I$. Se pusermos $A := I/I^0$ e $B = D/D^0$, então A e B são grupos abelianos de ordem prima com p e A é cíclico.

A inclusão natural $I \subset D$ induz uma injeção $A \hookrightarrow B$. Usando o teorema de Schur–Zassenhaus (o teorema 3 de I-3) podemos encontrar um levantamento $A \hookrightarrow I$

e um levantamento compatível $B \hookrightarrow D$. Fixemos de uma vez tais levantamentos e identifiquemos A com sua imagem em I e B com sua imagem em D. Obtemos então os produtos semidiretos: $I = A \propto I^0$ e $D = B \propto D^0$.

Seja K_v o corpo intermediário na extensão $\overline{Q}_p/Q_p$ que é o corpo fixo do morfismo natural $G_{Q_p} \to B$, de modo que $\mathrm{Gal}(K_v/Q_p) \cong B$, e seja L/L_z a extensão Galoisiana correspondente ao grupo de decomposição $\overline{\rho}(D)$. Nesta última subextensão tomo K/L_z, onde K é o corpo fixo pelo kernel da sobrejeção $\overline{\rho}(D) \to B$. Assim, $\mathrm{Gal}(K/L_z) \cong B$ e L/K tem grau 1*. Denotando por L_p o completamento de L (relativo à escolha inicial que fizemos, $\overline{Q} \hookrightarrow \overline{Q}_p$), temos que K_v é o completamento de K.

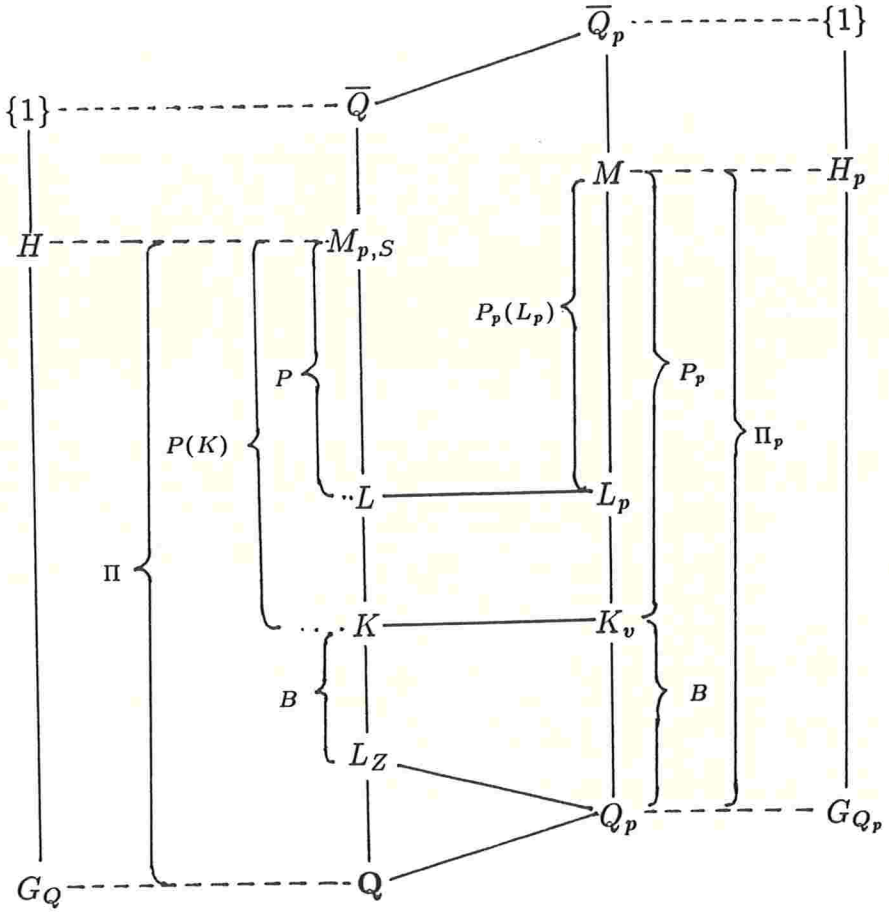
Seja $M_{p,S}/L$ a maior pro–p–extensão de L não ramificada fora de S e M/K_v a maior pro–p–extensão de K_v. Utilizaremos a seguinte notação adicional:

$$\Pi_p = \mathrm{Gal}(M/Q_p) \qquad \Pi = \mathrm{Gal}(M_{p,S}/Q)$$
$$P_p = \mathrm{Gal}(M/K_v) \qquad P = \mathrm{Gal}(M_{p,S}/L)$$
$$P(K) = \mathrm{Gal}(M_{p,S}/K),$$

Toda a informação dada acima, bem como as notações empregadas para os grupos de Galois podem ser visualizadas de uma vez no diagrama abaixo:

---

* De fato, com a hipótese de que $\overline{\rho}$ é moderadamente ramificada, $L = K$. Manteremos a notação distinta, pois no caso geral $L = K$ ou $[L : K] = p$ e nossos resultados são um pouco mais gerais.



No diagrama acima, as linhas pontilhadas indicam a correspondência de Galois nos casos local e global, e as linhas cheias inclinadas indicam o processo de completamento.

A injeção $v : G_{Q_p} \hookrightarrow G_Q$ induz naturalmente

$$\widetilde{v} : \Pi_p \to \Pi$$

e portanto $D = \widetilde{v}(\Pi_p)$. Novamente pelo teorema de Schur-Zasenhaus $\Pi_p = B \propto P_p$, onde $\widetilde{v} = (P_p) = D^0$ e analogamente $\widetilde{v}(I^{\text{sel}}) = I^0$, onde I^{sel} é a pro–p–parte da inércia na extensão M/Q. Vamos precisar aqui do seguinte lema, que se encontra em [Ma2] e cuja prova incluiremos aqui por ser essencial à compreensão do que segue:

Lema 1. Existem elementos $r, s \in I^0$ e $t \in D^0$ com as seguintes propriedades:

(1) O subgrupo $B \subset D$ está no centralizador de t.

(2) Se K_v não contiver as raízes p–ésimas da unidade, o elemento s é trivial. Caso contrário, ele satisfaz a seguinte relação:

para $g \in B$,

$$g\, s\, g^{-1} = s^{e(g)},$$

onde $e : B \to \mathbf{Z}_p^*$ é o levantamento de Teichmüller do carácter ciclotômico $\chi : B \to \mathbf{F}_p^*$ que define a ação natural de B no subgrupo das raízes p–ésimas da unidade em K_v.

(3) Os elementos $\{r^g = g\, r\, g^{-1}\ (g \in B),\ s \,e\, t\}$ geram D^0 como pro–p–grupo.

(4) O subgrupo normal fechado gerado pelos elementos $\{r^g\ (g \in B)\ e\, s\}$ é igual a I^0.

Prova: Como é bem conhecido, o quociente de p–Frattini de G_{K_v} é isomorfo, como $\mathbf{F}_p[B]$–módulo, a $K_v^*/(K_v^*)^p$ e a imagem da inércia é o subgrupo U_v/U_v^p, onde U_v é o grupo de unidades locais de K_v, e temos a seqüência exata de $\mathbf{F}_p[B]$–módulos:

$$0 \longrightarrow U_v/U_v^p \longrightarrow K_v^*/(K_v^*)^p \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow 0,$$

onde a ação de B em $\mathbf{Z}/p\mathbf{Z}$ é a ação trivial. Essa seqüência cinde, e o $\mathbf{F}_p[B]$–módulo U_v/U_v^p é isomorfo à soma direta da representação regular $\mathbf{F}_p[B]$ e de $\boldsymbol{\mu}_p(K_v)$, o grupo das raízes p–ésimas da unidade em K_v. Se K_v não contiver raízes p–ésimas da unidade, então $U_v/U_v^p \cong \mathbf{F}_p[B]$.

Assim, podemos encontrar três elementos $\overline{x}$, $\overline{y}$ e $\overline{z}$ no quociente de p–Frattini de G_{K_v} com as seguintes propriedades:

(i) O elemento $\overline{z}$ é fixo sob a ação de B (i.e., $\overline{z} \in \mathbf{Z}/p\mathbf{Z}$).

(ii) Os elementos $\overline{x}$ e $\overline{y}$ estão em U_v/U_v^p e esse subespaço é gerado por $\{g\cdot\overline{x}\ (g \in B)$ e $\overline{y}\}$.

(iii) O elemento $\overline{y}$ é trivial se K_v não contiver raízes p–ésimas não triviais da unidade; caso contrário é um autovetor da ação de B, que age como o carácter ciclotômico.

(iv) O quociente de p–Frattini de G_{K_v}, $K_v^*/(K_v^*)^p$, pode ser gerado pelos elementos $\{g \cdot \overline{x},\ (g \in B),\ \overline{y}\ \text{e}\ \overline{z}\}$.

Pelo teorema 4 de I-3 podemos encontrar levantamentos y, z em P_p, de $\overline{y}$, $\overline{z}$ respectivamente, que satisfazem a propriedade (1) e a relação de comutação da propriedade (2) do lema 1. (Veja especialmente os exemplos que se seguem ao teorema 4, em I-3). Para completar a prova da propriedade (2) do lema, precisamos mostrar que $y \in I^{\text{sel}}$. De fato, como P_p/I^{sel} é fixo pela ação de B, a projeção de y em P_p/I^{sel} é ao mesmo tempo fixa por B e verifica a relação de comutação de (2). Ora, como $\det\overline{\rho} \neq 1$, decorre que $y \in I^{\text{sel}}$.

Tomemos agora um levantamento x em I^{sel}, de $\overline{x}$. Pelo teorema de Burnside (veja a proposição 2 em I-3), o conjunto formado pelos elementos $\{x^g\ (g \in B),\ y\ \text{e}\ z\}$ geram P_p, donde a propriedade (3). Seja agora J o subgrupo normal fechado de P_p gerado por $\{x^g,\ (g \in B),\ \text{e}\ y\}$. Então $J \subseteq I^{\text{sel}}$ e P_p/J é gerado por um único elemento, a imagem de z. Assim, $P_p/J \to P_p/I^{\text{sel}} \cong \mathbf{Z}_p$ é um isomorfismo, e portanto $J = I^{\text{sel}}$. Pondo $r = \widetilde{v}(x)$, $s = \widetilde{v}(y)$ e $t = \widetilde{v}(z)$, obtemos o lema 1.

C.Q.D.

O próximo teorema é crucial na demonstração do teorema principal.

Teorema 1. O elemento $s \in I^0$, quando restrito a maior extensão p–abeliana elementar de L, é a identidade.

Prova: Se K_v não contiver as raízes p–ésimas da unidade isso é claro, pois podemos tomar o próprio s como a identidade, segundo (2) do lema 1. Vamos portanto supor que K_v contém uma raiz p–ésima ζ_p, não trivial, da unidade. A prova consistirá de vários passos, que ao se desenvolverem darão a estrutura da demonstração.

Antes de iniciarmos a prova, fixemos algumas notações. Se F for um corpo, $F^{\text{ab,p}}/F$ denotará a maior pro–p–extensão abeliana de F. Se F for um corpo de números, $F_S^{ab,p}/F$

denotará a maior pro–p–extensão abeliana de F que é não ramificada fora de $S = \{p, \infty\}$. Poremos também $H = Q(\zeta_p)$, $H_p = Q_p(\zeta_p)$ (isto é, o completado de H relativo a nossa escolha $\overline{Q} \hookrightarrow \overline{Q}_p$) $\mathcal{L}_p = \mathrm{Gal}(H_p^{ab,p}/H_p)$ e $\mathcal{L} = \mathrm{Gal}(H_S^{ab,p}/H)$. Observe-se que em se tratando da pro–p–extensão ciclotômica, $H^{ab,p} = H_S^{ab,p}$). Se Ω for um grupo profinito, escreveremos Ω^{ab} para o seu abelianizado, isto é, o quociente de Ω pelo subgrupo dos seus comutadores.

Passo 1: O seguinte diagrama é comutativo:

$$\begin{array}{ccc} P(K)^{ab} & \xleftarrow{\widetilde{v}} & P_P^{ab} \\ \uparrow \text{Ver.} & & \uparrow \text{Ver.} \\ \mathcal{L} & \xleftarrow{\widetilde{v}} & \mathcal{L}_P \end{array}$$

onde Ver. é o homomorfismo de transferência, ou "transfer map", ou ainda "Verlagerung", como é usualmente chamado.

Prova do Passo 1: Da teoria global dos corpos de classes temos a comutatividade do seguinte diagrama:

$$\begin{array}{ccc} C_H & \xrightarrow{\psi_H} & \mathrm{Gal}(H^{ab}/H) \\ \downarrow \text{Con.} & & \downarrow \text{Ver.} \\ C_K & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

onde C_H e C_K são os grupos de classes de idéles de H e K respectivamente, e ψ_H e ψ_K são os homomorfismos de Artin globais – ver [Ta]. Como estamos interessados em extensões que não ramificam fora de S, posso substituir os grupos de Galois no diagrama acima pelos

seus respectivos quocientes: $\mathrm{Gal}(H_S^{ab}/H)$ e $\mathrm{Gal}(K_S^{ab}/K)$ e considerar o homomorfismo de transferência induzido (continuaremos a chamá-lo de Ver.), cuja descrição explícita daremos a seguir.

Como $\mathrm{Gal}(H_S^{ab}/H) = \varprojlim_{\mathcal{F}} \mathrm{Gal}(F_S/H)$, onde $\mathcal{F}$ é o conjunto das extensões abelianas finitas F_S/H não ramificadas fora de S, posso substituir $\mathcal{F}$ por qualquer parte cofinal a $\mathcal{F}$, como por exemplo $\{H_m\}_{m\geq 0}$, onde H_m é o corpo de raio módulo $p^{n+1}\mathcal{O}_H$ (aqui $\mathcal{O}_H$ denota o anel de inteiros de H). Se pusermos $G_m(H) = \mathrm{Gal}(H_m/H)$, então

$$\mathrm{Gal}(H_S^{ab}/H) = \varprojlim G_m(H).$$

Se $J(H)$ denota o grupo de classes de ideais primos com p e $P_m(H)$ o raio módulo $p^{m+1}\mathcal{O}_H$ temos (ver [Neu]):

$$G_m(H) \cong J(H)/P_m(H).$$

Se $\sigma \in \mathrm{Gal}(H_S^{ab}/H)$, σ é representado pela família de suas restrições σ_m a H_m. Utilizando o símbolo de Artin, podemos escrever:

$$\sigma_m = \left(\frac{H_m/H}{\eta_m}\right),$$

onde $\eta_m \in J(H)$ e vale a relação de compatibilidade:

$$\eta_{m+1} \in \eta_m P_m(H) \quad (m \geq 0)$$

Podemos então pôr:

$$\sigma = \left(\left(\frac{H_m/H}{\eta_m}\right)\right)_m$$

e o homomorfismo de transferência Ver.: $\mathcal{L} \to P(K)^{ab}$ pode ser dado explicitamente:

$$\mathrm{Ver.}\left(\left(\frac{H_m/H}{\eta_m}\right)\right)_m = \left(\left(\frac{K_m/K}{\eta_m \mathcal{O}_K}\right)\right)_m .$$

Da teoria local dos corpos de classe temos a comutatividade do seguinte diagrama:

$$\begin{array}{ccc} H_p^* & \xrightarrow{\theta_{H_p}} & \mathrm{Gal}(H_p^{ab}/H_p) \\ \Big\downarrow \text{incl.} & & \Big\downarrow \text{Ver.} \\ K_v^* & \xrightarrow{\theta_{K_v}} & \mathrm{Gal}(K_v^{ab}/K_v) \end{array}$$

onde os θ's são os homomorfismos de reciprocidade local – cf. [Se].

Para provar o passo 1, precisamos reunir os dois diagramas anteriores, isto é, precisamos da compatibilidade entre a teoria local e a teoria global dos corpos de classes, e para tanto, consideraremos a injeção canônica

$$[\,] : K_v^* \to C_K$$

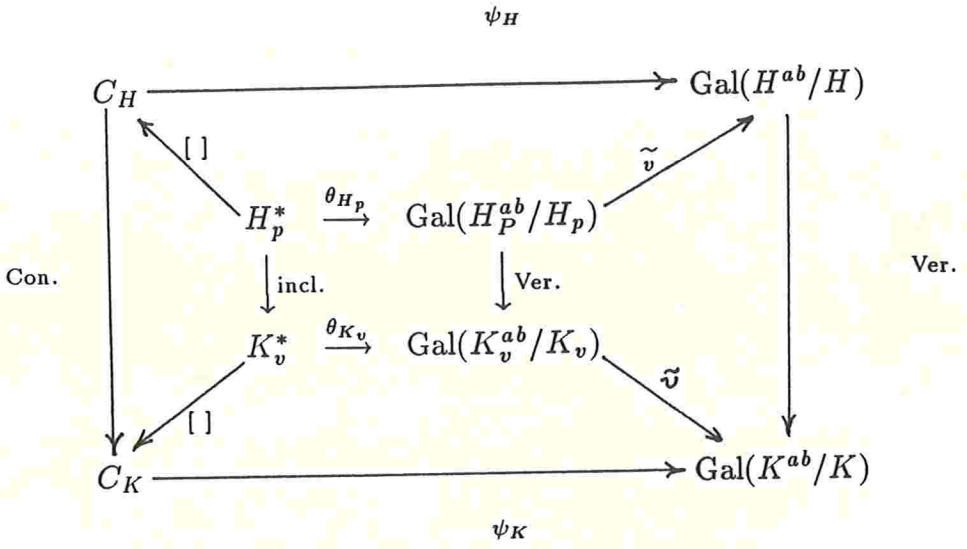
que a cada $a_v \in K_v^*$ associa a classe do idéle

$$[a_v] = (\ldots 1, 1, a_v, 1, 1, \ldots) \; .$$

A compatibilidade aludida acima reflete-se na comutatividade do diagrama abaixo (ver [Neu]):

$$\begin{array}{ccc} K_v^* & \xrightarrow{\theta_{K_v}} & \mathrm{Gal}(K_v^{ab}/K_v) \\ \Big\downarrow [\,] & & \Big\downarrow \widetilde{v} \\ C_K & \xrightarrow{\psi_K} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

Observemos que temos um outro diagrama comutativo análogo a esse, com H no lugar de K e H_p no lugar de K_v. A junção de todos esses diagramas nos fornece:



Como os θ's são epimorfismos, o trapézio da direita comuta. Projetando os grupos de Galois globais nos seus quocientes e tomando os p-Sylows, obtemos o diagrama comutativo:

$$\begin{array}{ccc} \mathrm{Gal}(H_p^{ab,p}/H) & \xrightarrow{\widetilde{v}} & \mathrm{Gal}(H_s^{ab,p}/H) \\ \Big\downarrow \text{Ver.} & & \Big\downarrow \text{Ver.} \\ \mathrm{Gal}(K_v^{ab,p}/K_v) & \xrightarrow{\widetilde{v}} & \mathrm{Gal}(K_s^{ab,p}/K) \end{array}$$

Isso prova o passo 1.

Passo 2. O elemento $y \in I^{\mathrm{sel}}$ (veja a prova do lema 1) pode ser escolhido de tal modo que a sua projeção y' em P_p^{ab} seja imagem através do "Verlagerung", de um elemento y'' em $\mathcal{L}_p$. Esse elemento y'' quando projetado no Frattini $\overline{\mathcal{L}}_p$ gera a componente $\boldsymbol{\mu_p}$.

Prova do Passo 2. Tomando o quociente de p–Frattini dos grupos que aparecem no diagrama da teoria local de corpos de classe, da página [60], obtemos:

$$\begin{array}{ccc} K_v^*/(K_v^*)^p & \xrightarrow{\cong} & \overline{P_p^{ab}} \\ & \overline{\theta}_{K_v} & \\ \uparrow \overline{\text{incl.}} & & \uparrow \overline{\text{Ver.}} \\ H_p^*/(H_p^*)^p & \xrightarrow{\cong} & \overline{\mathcal{L}_p} \\ & \overline{\theta}_{H_p} & \end{array}$$

Não é difícil ver que o homomorfismo induzido pela inclusão, $\overline{\text{incl}} : H_p^*/(H_p^*)^p \to K_v^*/(K_v^*)^p$ é injetor. De fato, se algum elemento α de H_p^* for uma potência p–ésima em K_p^*, $\alpha = \beta^p$ para certo $\beta \in K_v^*$, então como H_p contém as raízes p–ésimas da unidade, o grau de $H_p(\beta)$ sobre H_p seria p se α não fosse uma potência p–ésima em H_p^*, mas p não divide o grau da extensão K_v/H_p, donde $\overline{\text{incl}}$ é injetor. Como os $\overline{\theta}$'s são isomorfismos, o morfismo de transferência induzido, $\overline{\text{Ver.}} : \overline{\mathcal{L}_p} \to \overline{P_p^{ab}}$ é injetor.

Se pusermos $\mathbf{G} = \text{Gal}(H_p/Q_p)$ então, como na prova do lema 1, podemos escrever:

$$\overline{\mathcal{L}_p} \cong \mathbf{F}_p[\mathrm{G}] \oplus \boldsymbol{\mu}_p \oplus \mathbf{F}_p$$

$$\overline{P_p^{ab}} \cong \mathbf{F}_p[B] \oplus \boldsymbol{\mu}_p \oplus \mathbf{F}_p$$

Tomo $\overline{y''} \in \overline{\mathcal{L}_p}$ um elemento que vai em $\overline{y} \in \overline{P_p} = \overline{P_p^{ab}}$ (o que é possível, pois $\overline{\text{Ver.}}$ é equivalente à $\overline{\text{incl.}}$) e ponho $y' = \text{Ver.}(y'')$. Então $y' \in P_p^{ab}$ e $\overline{y}' = \overline{y}$, o que prova o passo 2.

Passo 3. Denotando por Φ a aplicação $\overline{\mathcal{L}_p} \to \mathcal{L}$ induzida nos Frattinis pelo homomorfismo $\widetilde{v} : \mathcal{L}_p \to \mathcal{L}$ temos que $\Phi(\overline{y}'') = 1$.

Prova do Passo 3. Consideremos a transformação de Artin global

$$\psi_H : I_H \longrightarrow \text{Gal}(H_S^{ab}/H)$$

onde I_H é o grupo de idéles de H. O kernel de ψ_H é o menor subgrupo fechado contendo H^* e $U_{[p]} \cdot I^\infty$, onde

$$U_{[p]} = \Pi_{\ell \neq p} \Pi_{\mathcal{P}/\ell} U_{\mathcal{P}} \quad \text{e} \quad I^\infty = \Pi_{\mathcal{P}/\infty} H_{\mathcal{P}}^*$$

e relembramos que $U_{\mathcal{P}}$ é o grupo de unidades no completado $H_{\mathcal{P}}$ de H em $\mathcal{P}$. Temos portanto a seqüência exata:

$$1 \longrightarrow \overline{U_{[p]} \cdot I^{\infty} \cdot H^*} \longrightarrow I_H \longrightarrow \mathrm{Gal}(H_S^{ab}/H) \longrightarrow 1$$

onde a barra acima indica o fecho na topologia dos idéles.

Como $H = Q(\zeta_p)$, só existe um primo $\mathcal{P}$ em H que divide p, e portanto escrevermos U_p em vez de $\Pi_{\mathcal{P}/p} U_{\mathcal{P}}$.

Temos as inclusões:

$$I_H \supseteq I_H^1 \cdot H^* = U_p \cdot \overline{U_{[p]} \cdot I^{\infty} \cdot H^*} \supseteq \overline{U_{[p]} \cdot I^{\infty} \cdot H^*} \, .$$

O primeiro quociente é isomorfo ao grupo de classes de ideais de H e o segundo é igual a:

$$U_p/(U_p \cap \overline{U_{[p]} \cdot I^{\infty} \cdot H^*}) \, .$$

Podemos dispor essas informações num diagrama comutativo:

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{U_{[p]}.I^{\infty}.H^*} & \longrightarrow & U_p.\overline{U_{[p]}.I^{\infty}.H^*} & \longrightarrow & \mathrm{Gal}(H_S^{ab}/\widehat{H}) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \overline{U_{[p]}.I^{\infty}.H^*} & \longrightarrow & I_H & \xrightarrow{\psi_H} & \mathrm{Gal}(H_S^{ab}/H) & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & I_H/I_H^1.H^* & \xrightarrow{\cong} & \mathrm{Gal}(\widehat{H}/H) & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

onde $\widehat{H}/H$ é a maior extensão abeliana não ramificada de H (o corpo de classes de Hilbert de H) e $\mathrm{Gal}(\widehat{H}/H)$ é isomorfo ao grupo de classes de ideais de H, denotado $\mathrm{Cl}(H)$.

Como $U_p \cap \overline{(U_{[p]} \cdot I^{\infty} \cdot H^*)} = \overline{E}$, o fecho das unidades globais de H diagonalmente imersas em U_p, o seguinte diagrama comuta:

$$\begin{array}{ccccccccc}
 & & U_p.\overline{U_{[p]}.I^{\infty}.H^*} & \xrightarrow{i} & I_H & & & & \\
 & \nearrow [\,] & & & & & & & \\
U_p & & \downarrow & & \downarrow \psi_H & & & & \\
 & \searrow [\,] & & & & & & & \\
1 & \longrightarrow & U_p/\overline{E} & \longrightarrow & \mathrm{Gal}(H_S^{ab}/H) & \longrightarrow & \mathrm{Cl}(H) & \longrightarrow & 1
\end{array}$$

Adicionando a esse diagrama a informação local, obtemos:

$$\begin{array}{ccccccccccc}
 & & & & U_p & \longrightarrow & H_p^* & \xrightarrow{\theta_{H_p}} & \mathrm{Gal}(H_p^{ab}/H_p) & & \\
 & & & & \downarrow \mathrm{id} & & \downarrow [\,] & & \downarrow \widetilde{v} & & \\
 & & & & U_p & \xrightarrow{\mathrm{io}[\,]} & I_H & \xrightarrow{\psi_H} & \mathrm{Gal}(H_S^{ab}/H) & & \\
 & & & & \downarrow \mathrm{id} & & & & \downarrow \mathrm{id} & & \\
1 & \longrightarrow & \overline{E} & \longrightarrow & U_p & \longrightarrow & & & \mathrm{Gal}(H_S^{ab}/H) & \longrightarrow & \mathrm{Cl}(H) \longrightarrow 1
\end{array}$$

Observe-se que como só existe um ideal primo $\mathcal{P}$ que divide p em H, o grupo das unidades locais em H_p coincide com U_p e isso é absolutamente crucial, pois na seqüência exata de baixo, $\overline{E}$ se inclui diagonalmente em $U_p = \Pi_{\mathcal{P}/p}.U_{\mathcal{P}}$, que no nosso caso reduz-se a U_p, e portanto a inclusão diagonal torna-se uma inclusão simples. Se tomarmos os p–Frattinis obteremos:

$$\begin{array}{ccccccccccc}
 & & & & U_p/U_p^p & \longrightarrow & H_p^*/(H_p^*)^p & \xrightarrow{\cong} & \overline{\mathcal{L}_p} & & \\
 & & & & \downarrow \mathrm{id} & & & & \downarrow \Phi & & \\
0 & \longrightarrow & B_S & \longrightarrow & B & \longrightarrow & U_p/U_p^p & \longrightarrow & \overline{\mathcal{L}} & \longrightarrow & \mathrm{Cl}(H)/\mathrm{Cl}(H)^p \longrightarrow 0
\end{array}$$

onde $B = \{x \in H^* : (x) = I^p\}/(H^*)^p$ e

$$B_s = \{x \in H^* : (x) = I^p,\ x \in (H_p^*)^p\}/(H^*)^p\ .$$

Preferimos, na seqüência exata dos p–Frattinis, utilizar a interpretação (e a notação) usual do pedaço que aparece à esquerda de $U_p/U_p^p \to \overline{\mathcal{L}} \to C/C^p \to 0$, que pode ser vista mais detalhadamente em [Koch] (Satz.11.7).

Se olharmos para esse diagrama como um diagrama de $\mathbf{F}_p[\mathbf{G}]$–módulos (recordo que $\mathbf{G} \cong \mathrm{Gal}(H_p/Q_p)$), veremos:

$$\begin{array}{ccccccccc} & & & & \mathbf{F}_p[\mathbf{G}] \oplus \boldsymbol{\mu}_p & \longrightarrow & \overline{\mathcal{L}}_p & & \\ & & & & \downarrow \mathrm{id} & & \downarrow \Phi & & \\ 0 & \longrightarrow & B_S & \longrightarrow & B & \longrightarrow & \mathbf{F}_p[\mathbf{G}] \oplus \boldsymbol{\mu}_p & \longrightarrow & \overline{\mathcal{L}} \longrightarrow C/C^p \longrightarrow 0 \end{array}$$

Como $\overline{y''} \in \boldsymbol{\mu}_p$ está na imagem de $B \to \mathbf{F}_p[\mathbf{G}] \oplus \boldsymbol{\mu}_p$ (pois B contém E/E^p e $\zeta_p \in E$), e não está na imagem de $B_s \to B$ (pois ζ_p não é potência p–ésima em H_p^*), da comutatividade do diagrama segue que $\Phi(\overline{y''}) = 1$.

Prova do teorema 1. Consideremos o diagrama abaixo:

$$\begin{array}{ccccccccc} & & & & P(K) & \xleftarrow{\widetilde{v}} & P_p & & \\ & & & \swarrow & \downarrow & & \downarrow & \searrow & \\ \overline{P(K)} & = & \overline{P(K)^{ab}} & \longleftarrow & P(K)^{ab} & \xleftarrow{\widetilde{v}} & P_p^{ab} & \longrightarrow & \overline{P_p^{ab}} \\ & & \uparrow \overline{\mathrm{Ver.}} & & \uparrow \mathrm{Ver.} & & \uparrow \mathrm{Ver.} & & \uparrow \overline{\mathrm{Ver}} \\ & & \overline{\mathcal{L}} & \longleftarrow & \mathcal{L} & \xleftarrow{\widetilde{v}} & \mathcal{L}_p & \longrightarrow & \overline{\mathcal{L}}_p \\ & & & \curvearrowleft & & \widetilde{\Phi} & & \curvearrowright & \end{array}$$

Relembramos que os elementos r, s, t em $P(K)$ são imagens de x, y, z em P_p e denotemos por r', s', t' e x', y', z' suas imagens nos abelianizados respectivos, $P(K)^{ab}$ e P_p^{ab}. Já vimos no passo 2 que $y' = \mathrm{Ver.}(y'')$ para certo $y'' \in \mathcal{L}_p$. Pelo passo 3 vemos que a imagem de $\widetilde{v}(y'')$ em $\overline{\mathcal{L}}$ é trivial. Pelo passo 1, o quadrado central comuta e portanto $s' = \mathrm{Ver}(\widetilde{v}(y''))$. Como o quadrado da esquerda é evidentemente comutativo, a projeção de s' no Frattini é trivial. Mas essa projeção é a mesma que a projeção de s em

$\overline{P(K)}$, donde s, restrito à maior extensão p–abeliana elementar de K é trivial. Como o grau de L/K é 1 ou p, L está contido nessa maior extensão p–abeliana elementar de K, e portanto s quando restrito a L é trivial. Em nosso caso, como supomos $\overline{\rho}$ moderadamente ramificada, $L = K$, e isso prova o teorema.

C.Q.D.

Prova do teorema principal. Vamos inicialmente provar a segunda parte do teorema, isto é, se $\overline{\rho}$ for moderadamente ramificada, então o kernel de $\mathbf{R} \to \mathbf{R}^0$ pode ser gerado por dois elementos (sairá também a sobrejetividade nesse caso!). E depois provaremos a sobrejetividade sem hipótese alguma.

Podemos supor (depois de realizar uma conjugação em $\overline{\rho}$, se necessário) que a imagem de $B \hookrightarrow D$ sob $\overline{\rho}$ é um subgrupo das matrizes diagonais em $GL_2(k)$ e que $A \subset B$ vai nas matrizes da forma

$$\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}.$$

A deformação universal de $\overline{\rho}$ pode ser vista como um homomorfismo

$$\rho : \Pi \to GL_2(\mathbf{R})$$

onde $\mathbf{R}$ é o anel universal das deformações de $\overline{\rho}$ e ρ é determinado a menos de equivalência estrita. Escolheremos um homomorfismo ρ, dentro da sua classe de equivalência estrita, de tal modo que a imagem de B esteja contida na imagem em $Gl_2(\mathbf{R})$ do subgrupo das matrizes diagonais de $GL_2(W(k))$ – onde o morfismo $GL_2(W(k)) \to GL_2(\mathbf{R})$ é induzido pelo morfismo natural $W(k) \to \mathbf{R}$. E podemos ainda arrumá-lo de modo que a imagem de A esteja na imagem do subgrupo das matrizes diagonais de $GL_2(W(k))$ da forma

$$\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}.$$

Sejam r, s, t os elementos de D^0 com as propriedades estipuladas no lema 1, e consideremos suas imagens sob ρ.

Lema 2. $\rho(s) = 1$.

Prova. Seja $u = \rho(s)$ e $\overline{u} \in GL_2(k)$ a sua redução módulo o homomorfismo induzido por $\mathbf{R} \to k$. Como ρ é um levantamento de $\overline{\rho}$, isto é, o seguinte diagrama é comutativo;

$$\begin{array}{ccc} & & GL_2(\mathbf{R}) \\ & \rho \nearrow & \\ \Pi & & \downarrow \\ & \overline{\rho} \searrow & \\ & & GL_2(k) \end{array}$$

então $\overline{u} = \overline{\rho}(s)$. Pelo teorema 1 acima, s quando restrito a L é trivial. Mas L é o corpo fixo por $\mathrm{Ker}\overline{\rho}$, donde $\overline{u} = 1$.

Para deduzir que $u = 1$, faremos um processo de indução: sejam $I_2 \subset I_1$ ideais em $\mathbf{R}$ e coloquemos $\mathbf{R}_j = \mathbf{R}/I_j$, $j = 1, 2$. Seja $u_j \in \mathbf{R}_j$ a projeção de u para $\mathbf{R}_j$. Supomos também que $m_{\mathbf{R}}.I_1 \subset I_2$, onde $m_{\mathbf{R}}$ é o ideal maximal de $\mathbf{R}$. Assim, o kernel da projeção $\mathbf{R}_2 \to \mathbf{R}_1$ possui naturalmente a estrutura de um k–espaço vetorial, que suporemos de dimensão 1, e portanto gerado por um único elemento, chamemo-lo ε', tal que $m_{\mathbf{R}} \cdot \varepsilon' = 0$. Supondo que $u_1 = 1$, provaremos que u_2 também é 1.

Escrevemos $u_2 = 1 + \varepsilon' M$ onde M é uma matriz 2×2 com entradas em k e $u_2 \in \Gamma_2(\mathbf{R}_2/\mathbf{R}_1)$, onde $\Gamma_2(\mathbf{R}_2/\mathbf{R}_1) = \ker(GL_2(\mathbf{R}_2) \to GL_2(\mathbf{R}_1))$.

Temos o seguinte diagrama comutativo:

$$\begin{array}{ccc} \Gamma_2(\mathbf{R}_2/\mathbf{R}_1) & \longrightarrow & \Gamma_2(k[\varepsilon]) \\ \downarrow & & \downarrow \\ GL_2(\mathbf{R}_2) & \longrightarrow & GL_2(k[\varepsilon]) \\ \nearrow & & \\ \Pi \quad \downarrow & & \downarrow \\ \searrow & & \\ GL_2(\mathbf{R}_1) & \longrightarrow & GL_2(k) \end{array}$$

onde os levantamentos $\Pi \to GL_2(\mathbf{R}_i)$ $i = 1, 2$ são induzidos das projeções $\mathbf{R} \to \mathbf{R}_i$ e o morfismo $GL_2(\mathbf{R}_2) \to GL_2(k[\varepsilon])$ é induzido por $\mathbf{R}_2 \to k[\varepsilon]$, e $k[\varepsilon] = \{a + \varepsilon b \mid a, b \in k,\ \varepsilon^2 = 0\}$. Observe-se que de fato $\Gamma_2(\mathbf{R}_2/\mathbf{R}_1)$ é isomorfo a $\Gamma_2(k[\varepsilon])$, via

$$1 + \varepsilon' M \mapsto 1 + \varepsilon M.$$

No diagrama acima, obtivemos uma representação de Π em $GL_2(k[\varepsilon])$, que levanta $\overline{\rho}$ e tal que o elemento $s \in I^0$ vai em $1 + \varepsilon M \in \Gamma_2(k[\varepsilon])$. É muito fácil ver que a multiplicação em $\Gamma_2(k[\varepsilon])$ resulta na adição componente a componente e portanto, $\Gamma_2(k[\varepsilon])$ é um grupo abeliano finito p–elementar. Isso significa que o corpo fixo do kernel de $\Pi \to GL_2(k[\varepsilon])$ me fornece uma extensão de L p–abeliana elementar. Ora, como s é trivial no $\overline{P(L)}$, então $M = 0$ e portanto $u_2 = 1$. Como $\mathbf{R} \in C(k)$, é possível construir uma seqüência de ideais $m_{\mathbf{R}} = \eta_1 \supset \eta_2 \supset \ldots$ tal que $\eta_j \supset \eta_{j+1}$ possui as propriedades requeridas para $I_2 \supset I_1$ e tal que $\cap \eta_j = 0$, concluímos que $u = \rho(s) = 1$. Isso termina a prova do Lema 2.

Continuando a prova do teorema principal, escreveremos $\rho(r) \in GL_2(\mathbf{R})$ como uma matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Como $\overline{\rho}$ é ordinária e normalizamos as coisas de modo que a imagem da inércia sob

$\overline{\rho}$ esteja contida no subgrupo da forma

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

temos que $(a-1)$ e c pertencem ao ideal maximal de $\mathbf{R}$. Formemos o quociente $\mathbf{R}' = \mathbf{R}/(a-1, c)$ e seja

$$\rho' : \Pi \to GL_2(\mathbf{R}')$$

o homomorfismo induzido de ρ pela projeção $\mathbf{R} \to \mathbf{R}'$. Por construção, r vai numa matriz da forma

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$$

em $GL_2(\mathbf{R}')$ sob ρ'. Qualquer um dos conjugados de r por elementos $g \in B$ terá a mesma forma da matriz de r acima, pois g vai numa matriz diagonal. Assim, pelo lema 2,

$$\rho'(I^0) \subseteq \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

Como $\overline{\rho}$ é moderadamente ramificada, e portanto $\det \overline{\rho} \neq 1$, segue que $\det \overline{\rho}$ é não trivial quando restrito a A. Segue da propriedade (1) do lema 1 que $\rho(t)$ é uma matriz diagonal em $GL_2(\mathbf{R})$ (e portanto em $GL_2(\mathbf{R}')$). Da propriedade (3) segue que D^0 vai no subgrupo de Barel

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

de onde temos a conseqüência que ρ' é ordinária. Existe portanto um único homomorfismo de anéis locais $\mathbf{R}^0 \to \mathbf{R}'$ tal que o diagrama comuta:

$$\begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R}' \\ & \searrow \quad \nearrow & \\ & \mathbf{R}^0 & \end{array}$$

Se $\rho^0 : \Pi \to GL_2(\mathbf{R}^0)$ denota o homomorfismo induzido por ρ, i.e., ρ^0 é um representante da deformação ordinária universal de $\overline{\rho}$, então ρ' é induzido de ρ^0 via $\mathbf{R}^0 \to \mathbf{R}'$. A segunda parte do teorema estaria provada mostrássemos que a vai em 1 e c vai em 0 sob $\mathbf{R} \to \mathbf{R}^0$, pois nesse caso teríamos um mapa $\mathbf{R}' \to \mathbf{R}^0$ (injetor, por sinal!) e a representação ρ', que já vimos ser ordinária, induziria ρ^0. Pela universalidade de $\mathbf{R}$, $\mathbf{R}^0 \cong \mathbf{R}'$ e $\rho' = \rho^0$.

Seja $M^0 = \mathbf{R}^0 \times \mathbf{R}^0$ considerado com a estrutura natural de Π–módulo via ρ^0 e a ação usual de GL_2. Observe-se que o sub-módulo em M^0 consistindo dos vetores fixos sob a ação de A é o $\mathbf{R}^0$–módulo livre de posto 1, $\mathbf{R}^0 \times 0 \subset M^0$. Como ρ^0 é ordinária, segue que $\mathbf{R}^0 \times 0$ tem que ser fixo por todo I^0 e, em particular, por r, ou seja, $a - 1$ e c vão em zero sob $\mathbf{R} \to \mathbf{R}^0$.

Resta provar a primeira parte do teorema, ou seja, que $\mathbf{R} \to \mathbf{R}^0$ é sobrejetor (note que obtivemos já a sobrejetividade supondo $\overline{\rho}$ moderadamente ramificada). Pelas nossas normalizações, podemos supor que o vetor fixo pela inércia em $k \times k$ é o vetor $(1, 0)$. Seja $(x, y) \in \mathbf{R}^0 \times \mathbf{R}^0$ um gerador do $\mathbf{R}^0$–submódulo livre de posto 1 e somando direto de $\mathbf{R}^0 \times \mathbf{R}^0$, que é fixo pela inércia via ρ^0. É claro que (x, y) projeta-se em $(1, 0)$ e portanto $x = 1 + \alpha$ e $y = \beta$, onde α e β pertencem ao ideal maximal de $\mathbf{R}^0$.

Afirmamos que podemos encontrar um homomorfismo $\widetilde{\rho^0}$ na classe de equivalência estrita de ρ^0, e tal que o sub $\mathbf{R}^0$–módulo dos invariantes por inércia seja $(1, 0) \in \mathbf{R}^0 \times \mathbf{R}^0$. De fato, se M for a matriz

$$M = \begin{pmatrix} 1 + \alpha & 0 \\ \beta & 1 \end{pmatrix},$$

então $M \in \Gamma_2(\mathbf{R}^0)$ e M leva o $\mathbf{R}^0$–módulo gerado por $(1, 0)$ no $\mathbf{R}^0$–módulo gerado por (x, y). Se pusermos

$$\widetilde{\rho^0} = M^{-1} \rho^0 M$$

então $\widetilde{\rho^0}$ é da mesma classe de equivalência de ρ^0 e a inércia fixa $(1, 0)$ via $\widetilde{\rho^0}$. Como $\widetilde{\rho^0}$ é ordinária, o submódulo $\mathbf{R}^0 \times 0$ é o fixo pela inércia e portanto, se $\mathbf{R}'$ denotar a

iamgem de $\mathbf{R} \to \mathbf{R}^0$, e ρ' a imagem da deformação universal induzida por $\mathbf{R} \to \mathbf{R}'$, basta provar que ρ' é ordinária para termos o resultado. Porém, $(1,0) \in \mathbf{R}' \times \mathbf{R}'$ é fixo pela inércia e portanto $\mathbf{R}' \times 0$ é lvire de posto 1, fixo pela inércia e somando direto de $\mathbf{R}' \times \mathbf{R}'$. Se algo mais fosse fixo pela inércia, teria que ser da forma $r \cdot (1,0)$, para certo $r \in \mathbf{R}^0$. Como estamos em $\mathbf{R}' \times \mathbf{R}'$, esse r tem que estar em $\mathbf{R}'$ e isso termina a prova da primeira parte do teorema, e o teorema principal está provado.

C.Q.D.

Corolário (cf. [Ma2]). Seja $\overline{\rho}$ uma representação residual ordinária moderadamente ramificada que não seja totalmente real. Então a dimensão de Krull de $\mathbf{R}^0/p\mathbf{R}^0$ é ≥ 1. Se a dimensão de Zanski de $\mathbf{R}^0/p\mathbf{R}^0$ for ≤ 1, então $\mathbf{R}^0$ é um anel de séries de potência em uma variável sobre $\mathbf{Z}_p$ e $\mathbf{R}$ é um anel de séries de potências em dois parâmetros sobre Λ.

Prova. O conjunto das deformações de $\overline{\rho}$ para $k[\varepsilon]$ que sejam ordinárias é naturalmente munido de uma estrutura de k–espaço vetorial (cf. [Sch]), que como tal é dual de $m_{\mathbf{R}^0}/(m_{\mathbf{R}^0}^2, p)$ (cf. [Ma1] ou [Bo]) e sua dimensão sobre k é chamada a dimensão de Zariski de $\mathbf{R}^0/p\mathbf{R}^0$. Como o corpo fixo de $\ker\overline{\rho}$ não é uma extensão totalmente real, $\mathbf{R}/p\mathbf{R}$ tem dimensão de Krull ≥ 3 (cf. [Ma1]) e pelo teorema principal, $\mathbf{R}^0/p\mathbf{R}^0$ é um quociente de $\mathbf{R}/p\mathbf{R}$ por um ideal gerado por dois elementos, donde a dimensão de Krull de $\mathbf{R}^0/p\mathbf{R}^0$ é ≥ 1. Suponhamos que a dimensão de Zariski de $\mathbf{R}^0/p\mathbf{R}^0$ seja ≤ 1. O nosso teorema principal implica que a dimensão de Zariski de $\mathbf{R}/p\mathbf{R}$ é ≤ 3. Por ([Ma1], Cor.3 à Prop.5, Chap.I, §10) segue que $\mathbf{R}$ é um anel local regular de dimensão de Krull igual a 4, e mais precisamente, um anel de séries formais de potências em dois parâmetros sobre Λ. Pelo teorema principal e pela hipótese na dimensão de Zariski de $\mathbf{R}^0/p\mathbf{R}^0$ segue que $\mathbf{R}^0$ é um anel local regular com dimensão de Krull igual a 2 e $p \in \mathbf{R}^0$ é um elemento regular, o que termina a prova do corolário.

C.Q.D.

REFERÊNCIAS

[Bour] N. Bourbaki. *Eléments de Mathématiques.* Algébre Commutative IX, Masson, Paris, 1983.

[Koch] H. Koch. *Galoissche Theorie des p–Erweiterungen.* Springer–Verlag, Berlin–Heidelberg–New York, 1970.

[K-L] N. Katz e S. Lang. "Finiteness Theorems in Geometric Classfield Theory". Enseign. Math. (2) 27 (1981), nº 3-4, 285-319 (1982).

[Sch] M. Schlessinger. "Functors of Artin Rings." Trans. A.M.S. 130 (1968), 208-222.

[Ma1] B. Mazur. "Deforming Galois Representation" em "Galois Groups over Q". Y. Ihara, K. Ribet, J.P. Serre, Eds. Springer–Verlag, Berlin/N.York.

[Bo] N. Boston. *Deformation Theory of Galois Representation.* Thesis. Harvard. 1987.

[Ro] D. Robinson. *A Course in the Theory of Groups.* Springer–Verlag, Berlin–Heidelberg–New York, 1982.

[Schi] G. Shimura. *Introduction of the Arithmetic of Automorphic Forms.* Princeton Univ. Press., Princeton N.J., 1971.

[De] P. Deligne. "Formes modulaires et representations l'àdiques." Seminaire Bourbaki 68/69, nº 355. Lecture Notes in Mathematics, 179, pp. 136-172. Springer–Verlag, 1971.

[De-Se] P. Deligne e J.P. Serre. "Formes modulaires de poids 1". Ann. Sci. Ec. Norm. Sup. 7 (1974), 507-530.

[Ma2] B. Mazur. "Two–dimensional p–adic Galois Representations unramified away from p". Compositio Mathematica 74: 115-133 (1990).

[M-W] B. Mazur e A. Wiles. "On p–Adic Analytic families of Galois Representations". Compositio Mathematica 59 (1986), 231-262.

[W] A. Wiles. "On ordinary λ–adic representations associated to modular forms". Inv. Math. 94, 529-573 (1988).

[H] H. Hida. "Iwasawa modules attached to congruences of cusp. forms". Ann. Sci. Ec. Norm. Snp 19 (1986).

[H2] H. Hida. "Galois Representations into $GL_2(\mathbf{Z}p[[T]])$ attached to ordinary cusp. forms". Inv. Math 85 (1986), 545-613.

[T] J. Tilouine. "Kummer's criterion over Λ and Hida's congruence Module". Hokkaido University Technical Report series in mathematics (1987).

[Goul] F.Q. Gouvea "Arithmetic of p–adic modular forms". Lecture Notes in Mathematics, 1304. Springer–Verlag, Berlin/N.York, 1988.

[M-T] B. Mazur e J. Tilouine. "Representations Galoisiennes Ordinaries et Differentielles de Kähler". Preprint.

[Ta] J. Tate. Global Class Field Theory. In Algebraic Number Theory, Cassels & Fröhlich Eds., 1967.

[Neu] J. Neukirch. Class Field Theory. Springer–Verlag. Berlin/N.York, 1986.

[Se] J.P. Serre. Local Class Field Theory. In Algebraic Number Theory, Cassels & Fröhlich. Eds. 1967.

[Gou2] F.Q. Gouvêa. "Controlling the Conductor". J.N.Theory.

[Bo-Ma] N. Boston e B. Mazur. "Explicit Universal Deformations of Galois Representations". Preprint.

[Bru] A. Brumer. "Galois Groups of Extensions of Algebraic Number Fields with given Ramification". Michigan. Math. J.B. (1966), 33-40.

[Serre] J.P. Serre. "Sur le représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{Q}/Q)$." Duke Math. J. 54 (1987), 179-230.

[Wa] L. Washington. "Introduction to Cyclotomic Fields". Springer–Verlag. Berlin–Heidelberg–New York, 1982.